

Index

- Δ_k^p 29, 72, 194, 271–273, 286, *see* hierarchy, polynomial, *see* set, Δ_2^p -complete
- Π_k^p 20, 25, 28, 271–273, *see* hierarchy, polynomial
- $\Pi_k^{p,C}$ 213, 214
- Σ_k^p 19–21, 25, 28, 73, 108, 271–273, *see* hierarchy, polynomial, *see* set, Σ_2^p -complete
- $\Sigma_k^{p,C}$ 213–216, 228
- Θ_k^p 18–20, 27, 29, 268, 271–273, 293, *see* hierarchy, polynomial, *see* set, Θ_2^p -complete
 - closure properties *see* closure, of Θ_k^p ...
- \leq_T^C 306
- \leq_T^L 83, 265, 306, 307, *see* reduction, logspace many-one
- $\leq_{\text{randomized}}$ 70, 72, 268, *see* reduction, randomized
- \leq_m^{comp} 241, 306, *see* reduction, coNP-many-one
- $\leq_T^{\text{NP} \cap \text{coNP}}$ 306
- $\leq_m^{p,A}$ 60, 284, 285
- \leq_T^p 1, 18–20, 22, 60, 182, 268, 269, 305, 306, *see* reduction, polynomial-time Turing
 - closure of C=P downward under *see* closure, of C=P downward under \leq_T^p
 - closure of coC=P downward under *see* closure, of coC=P downward under \leq_T^p
 - closure of $\oplus P$ downward under *see* closure, of $\oplus P$ downward under \leq_T^p
- \leq_{btt}^p 1, 8–11, 26, 268, 296, 298, 306–308, *see* reduction, polynomial-time bounded-truth-table
 - closure of P downward under *see* closure, of P downward under \leq_{btt}^p
 - closure of PP downward under *see* closure, of PP downward under \leq_{btt}^p
- \leq_c^p 306, *see* reduction, polynomial-time conjunctive Turing
- \leq_{ctt}^p 26, 187, 260, 305, *see* reduction, polynomial-time conjunctive truth-table
 - closure of C=P downward under *see* closure, of C=P downward under \leq_{ctt}^p
 - closure of coNP downward under *see* closure, of coNP downward under \leq_{ctt}^p
- \leq_d^p 306, *see* reduction, polynomial-time disjunctive Turing
- \leq_{dtt}^p 26, 29, 268, 305, 307, *see* reduction, polynomial-time disjunctive truth-table
 - closure of C=P downward under *see* closure, of C=P downward under \leq_{dtt}^p
 - closure of coNP downward under *see* closure, of coNP downward under \leq_{dtt}^p
- $\leq_{f(n)-T}^p$ 306
- $\leq_{f(n)-\text{tt}}^p$ 306
- $\leq_{k-\text{tt}}^p$ 10, 11, 245, 275, 306, *see* \leq_{btt}^p , *see* reduction, polynomial-time bounded-truth-table
- \leq_{locpos}^p 306, 307, *see* reduction, polynomial-time locally positive Turing
- \leq_m^p 1–6, 8, 9, 26, 60, 187, 194, 245, 267–269, 275, 305, *see* reduction, polynomial-time many-one
 - closure of PP downward under *see* closure, of PP downward under \leq_m^p
 - closure of SF₅ downward under *see* closure, of SF₅ downward under \leq_m^p
 - closure of the context free languages downward under *see* closure, of the context free languages downward under \leq_m^p

- \leq_{pos}^p 296, 306, 307, *see* reduction, polynomial-time positive Turing
- closure of $C=P$ downward under *see* closure, of $C=P$ downward under \leq_{pos}^p
- closure of $coC=P$ downward under *see* closure, of $coC=P$ downward under \leq_{pos}^p
- closure of NP downward under *see* closure, of NP downward under \leq_{pos}^p
- closure of P-sel downward under *see* closure, of P-sel downward under \leq_{pos}^p
- \leq_{tt}^p 248, 251, 260, 296, 305, *see* reduction, polynomial-time truth-table
- closure of PP downward under *see* closure, of PP downward under \leq_{tt}^p
- $\leq_{tt[k]}^p$ 249, 251, *see* reduction, polynomial-time constant-round truth-table
- \leq_T^{sn} 306, *see* reduction, strong nondeterministic
- $\oplus E$ 28
- $\oplus L$ 82, 87, 89, 277, 280, *see* class, modulo-based, logspace-analogs
- $\oplus L/poly$ 82, 89, *see* advice
- $\oplus OptP$ 181, 183, 192, 303
- $\oplus P$ 28, 72, 73, 76–82, 97, 101, 181–183, 185, 186, 194, 213, 232, 259, 273, 276, 277, 287, 289, 293, 297, 298, 301
- closure properties *see* closure, of $\oplus P\dots$
- exponential-time analog of *see* analog, exponential-time, of $\oplus P$, *see* analog, exponential-time, of UP, FewP, $\oplus P$, ZPP, RP, or BPP
- $\oplus P/poly$ 78, 82, *see* advice
- $\oplus SAT$ 298, *see* computation, modulo-based
- $\#L$ 87, 253, 279, *see* set, $\#L$ -complete
- $\#P$ 76, 78–81, 87, 88, 91–108, 110, 112–115, 119, 121, 163, 164, 237, 238, 240, 265, 273, 276, 286, 287, 289, 293, 297, 299, *see* class, counting, *see* function, $\#P$, *see* set, $\#P$ -complete
- closure properties *see* closure, of $\#P\dots$
- $\#P$ function *see* function, $\#P$
- $\#P_1$ 287
- $\#SAT$ 286
- $\#acc_N(x)$ 76, 77, 79–81, 121, 186, 187, 236–238, 251–253, 256–258, 278, 286, 290, 291, 297, 298
- $\#gap_N(x)$ 186, 236, 238, 239, 253, 254, 256, 258, 259, *see* function, GapP, *see* function, gap, *see* GapP
- $\#rej_N(x)$ 186, 187, 236–238, 258, *see* path, rejecting computation
- 2-ary function *see* function, ...2-ary...
- 2-disjunctively self-reducible set *see* set, 2-disjunctively self-reducible
- 3-CNF formula *see* formula, 3-CNF
- Abadi, M. 64, 164
- AC, AC^k 88, 193, 194, 261, 279–281, 293, 301, 308, *see* class, circuit
- ACC 193, 194, *see* class, circuit
- acceptance
 - cardinality *see* cardinality, acceptance
 - categorical 283
 - mechanism *see* mechanism, acceptance
 - probability *see* probability, acceptance
 - type *see* reduction, of the cardinality of acceptance types, *see* type, acceptance, *see* type, finite-cardinality acceptance
- access
 - k -round parallel 249
 - parallel, to NP 18, 64, 89, 301
 - sublinear-parallel, to NP 64
- ACC_p 88, *see* class, circuit
- Adachi, A. 264, 265
- addition
 - closure of $\#P$ under *see* closure, of $\#P$ under addition
- adjacency matrix *see* matrix, adjacency
- Adleman, L. 87, 277, 289, 290
- adversary problem *see* problem, adversary
- advice 45, 48, 84, 86, 87, 277, *see* $C/poly$, *see* $coNP/linear$, *see* $coNP/poly$, *see* $E/linear$, *see* $EXP/linear$, *see* interpreter, *see* $NL/poly$, *see* $NP/linear$, *see* $NP/poly$, *see* $(NP \cap coNP)/poly$, *see* $P/linear$, *see* $P/poly$, *see* $P/quadratic$, *see* $\oplus L/poly$, *see* $\oplus P/poly$, *see* $PP/linear$, *see* set, small advice, *see* $UL/poly$
- for the semi-feasible sets 47–56
- hard to compute 277
- linear-sized 49, 51, 52
- optimal 48, 52

- quadratic length-bounded 48
- subquadratic length-bounded 49
- advice interpreter *see* interpreter, advice
- Agrawal, M. 296, 298
- agreement
 - secret-key 36, 43
- Aho, A. 266
- Ajtai, M. 232, 280
- algorithm
 - census-based 18
 - deterministic exponential-time 24
 - enumeration 119
 - greedy 272
 - high-degree polynomial-time 264
 - interval-pruning vii
 - low-degree polynomial-time 266
 - membership 294
 - nondeterministic 1, 76, *see* NP, *see* Σ_k^p
 - NP 62, *see* NP, *see* Σ_k^p
 - polynomial-time 3, 5, 6, 22, 23, 25, 41, 80, 139, 146, 165, 266
 - query simulation vii
 - randomized 67
 - sampling 131, 132, 135, 136, 145–147, 149
 - self-reducibility 1
 - semi-membership 294, 295
 - Σ_2^p 20, 21, *see* Σ_k^p
 - that assumes a theorem’s hypothesis 1, 2
 - Θ_2^p 19, 20, *see* Θ_k^p
 - tree-pruning vii, 8
 - UL 85, 86, *see* UL
- algorithms
 - design and analysis of 265, 266
 - their central role in complexity theory vii, 1
- Allender, E. viii, 28, 29, 43, 88, 89, 231, 260, 261, 265, 270, 278, 279, 281, 283–285, 293, 308
- almost polynomial-time set *see* set, almost polynomial-time
- alphabet 7
- alternating quantifiers *see* quantifiers, alternating
- alternating Turing machine *see* machine, alternating
- alternation
 - symmetric 27
- AM 300
- Ambainis, A. ix, 194
- Amir, A. 63, 163, 286, 296, 297
- analog
 - exponential-time, of $\oplus P$ 28
 - exponential-time, of the polynomial hierarchy 28, 29
 - exponential-time, of UP, FewP, $\oplus P$, ZPP, RP, or BPP 28
- AND circuits *see* circuits, AND
- AND gate *see* gate, AND
- AND-OR circuits *see* circuits, AND-OR
- Angluin, D. 87
- Antioch
 - Holy Hand Grenade of 67
- aperiodic monoid *see* monoid, aperiodic
- approach
 - census 18
 - self-reducibility-based tree-pruning 2
 - theorems via algorithms under hypotheses 1
- approximation *see* factor, of approximation, *see* nonapproximability
 - enumerative 119, 163
 - NP-hardness of 166
 - of perm 119, *see* permanent, of a matrix
 - of maximum clique 165, 166, *see* clique
 - of #P functions 286
 - of the proper subtraction of two #P formulas 108
 - of the sign function 235, 242
 - of threshold circuits by parity circuits 260
- argument
 - self-reducibility-based 4
- arithmetic characterization *see* characterization, arithmetic
- arithmetic expression *see* expression, arithmetic
- arithmetic formula *see* formula, arithmetic
- arithmetization 111, 112, 126, 140, 163
- Arora, S. 165, 166, 267, 269
- Arthur-Merlin *see* AM
- Arvind, V. ix, 27, 277, 289, 296, 298
- Aspnes, J. 289
- assignment
 - exactly one satisfying 69
 - lexicographically largest satisfying 163

- lexicographically smallest satisfying 57
- partial 199
- random, partial input 197
- satisfying 4, 7, 56–59, 139, 163, 268, 269, 283, 294
- unique satisfying 45, 56, 57, 284
- assignments
 - even number of satisfying 298
 - number of satisfying 286
- associative operation *see* operation, associative
- associativity *see* function, ...associative..., *see* function, associativity of
 - of concatenation 38
 - of multiplication 38
 - weak 44
- attribute-value description *see* description, attribute-value
- Ausiello, G. 166, 267
- automata *see* machine
 - k -state 302
 - nondeterministic auxiliary pushdown 281
 - nonuniform deterministic finite 193, *see* NUDFA
 - pushdown 281
- automorphism *see* graph, automorphism counting in
 - counting in graph 289
- average-case cryptography *see* cryptography, average-case

- Babai, L. 28, 163–165, 232, 273, 300
- Baker, T. 231, 268–270, 272, 273
- Balcázar, J. 27, 43, 64, 87, 273, 286, 287, 293
- Barrington, D. 192–194, 281, 302
- Beals, R. 261, 278, 279, 289
- Beame, P. 233
- Beaver, D. 163
- behavior
 - normal 28, 29
- Beigel, R. ix, 29, 43, 63, 89, 106–108, 163, 194, 260, 269, 284, 286, 293, 296–298, 308
- Bellare, M. 166
- Ben-Or, M. 164, 194, 300
- Bennett, C. 87, 232, 268, 269
- Bent, R. viii
- Berg, C. 232
- Berman, L. 26, 27, 43, 269, 275–277, 282
- Berman, P. 26, 27
- Berman–Hartmanis Isomorphism Conjecture *see* Conjecture, Berman–Hartmanis Isomorphism
- Bertoni, A. 286
- Beygelzimer, A. viii, 44
- Bibliographic Notes *see* Notes, Bibliographic
- bidirectional connectivity *see* connectivity, bidirectional
- bijection 168
 - between natural numbers and strings 91, 92
 - between strings and pairs of strings 33
- binary tree
 - full *see* tree, full binary
- bits
 - a probabilistic circuit’s random 219
 - generation of random 289
 - quadratic number of random 88
 - quasilinear number of random 88
 - random, of a probabilistic circuit 220, 221
- blackboard
 - polynomial-sized 274
- Blackburn, P. 274
- Blass, A. 283
- Blaylock, N. ix
- Blum, M. 164
- Book, R. 27, 64, 65, 87, 273–275, 286, 287, 293, 294
- boolean formula *see* formula, boolean
- boolean formula minimization problem *see* problem, boolean formula minimization
- boolean function *see* function, ...boolean...
- boolean hierarchy *see* hierarchy, boolean
- boolean operation *see* operation, boolean
- Boppana, R. 269
- Borchert, B. 285
- Borodin, A. 193, 269, 279, 280
- bottleneck machine *see* machine, ...bottleneck...
- bound
 - lower 43, 44, 194, 197, 207, 223, 232, 233, 248, 264
 - quadratic 264
 - superpolynomial-size lower 264
- bounded

- depth of recursion 17
- polynomial-time 145, 182, 187, 192
- bounded-depth circuits *see* circuits, bounded-depth
- bounded-fan-in circuits *see* circuits, bounded-fan-in
- bounded-width branching program *see* program, bounded-width branching
- boundedness
 - logarithmic-space 85, 86, 254, 255, 258, 259, *see* L, *see* NL, *see* UL
 - polynomial-space 125, *see* PSPACE
 - polynomial-time 7, 12, 80, 81, 115, 118, 119, 121, 122, 135, 187, 238, 239, 246, 250, 255, 259, *see* machine, nondeterministic polynomial-time, *see* NP, *see* P
- Boutell, M. viii
- Bovet, D. ix, 268, 285
- BP operator *see* operator, BP
- BPP 28, 72–75, 77, 78, 81, 87, 273, 276, 277, 288–290, 293, 297, 298, 307, 308, *see* circuits, small for BPP
 - exponential-time analog of *see* analog, exponential-time, of UP, FewP, \oplus P, ZPP, RP, or BPP
- BPP hierarchy *see* hierarchy, BPP
- branching program *see* program, branching
- branching time logic *see* logic, branching time
- Brassard, J. 43
- Brauer, W. ix
- Braunmühl, B. von *see* von Braunmühl, B.
- Bruschi, D. 232, 297
- brute-force search *see* search, brute-force
- Bshouty, N. 27
- Buhrman, H. 28, 64, 273, 284, 296, 308
- Buhrman–Hemaspaandra–Longpré Encoding *see* Encoding, Buhrman–Hemaspaandra–Longpré
- Buntrock, G. 87, 277, 278
- Burtschick, H. 64, 296
- \mathcal{C}/poly 75, *see* advice
- $C=L$ 261, 278, 279, *see* set, $C=L$ -complete, *see* set, complete for the \leq_{tt}^L -reducibility closure of $C=L$
- $C=L$ hierarchy *see* hierarchy, $C=L$
- $C=L$ oracle hierarchy *see* hierarchy, oracle, of $C=L$
- $C=P$ 87, 88, 102, 103, 186, 187, 191, 192, 235, 240, 241, 260, 261, 287, 290–293, 298, 308, *see* class, counting, *see* set, $C=P$ -complete
 - closure properties *see* closure, of $C=P$...
- Cai, J. ix, 26, 27, 29, 64, 106, 107, 163, 164, 192, 194, 232, 265, 273–275, 286, 297, 298, 303
- call
 - recursive 14–18, 124, 125
- Canetti, R. 27
- cardinality
 - acceptance 102, 292
 - rejection 102
- cardinality reduction *see* reduction, of numbers of solutions, *see* reduction, of numbers of witnesses, *see* reduction, of the cardinality of a set of vectors, *see* reduction, of the cardinality of acceptance types, *see* reduction, of the number of accepting paths, *see* reduction, of the number of solutions, *see* reduction, witness
- Carroll, L. 272
- Cass, D. ix
- cat and mouse game *see* game, cat and mouse
- categorical acceptance *see* acceptance, categorical
- categorical machine *see* machine, categorical
- cauldrons
 - of recursion theory vii
- Caussin, H. 194, 260
- census *see* approach, census
- census function *see* function, census
- census value *see* value, census
- census-based algorithm *see* algorithm, census-based
- certificate
 - deterministically verifiable 109
 - of acceptance or membership 8, 9, 34, 62, 109
 - of primality 131, 132, 142
 - polynomial-time verifiable 131
 - succinct 109, 110
- Chakaravarthy, V. 64
- Chandra, A. 193, 272, 279, 281, 308
- Chang, R. 231, 260, 270, 289, 300, 308
- characteristic function *see* function, characteristic
- characterization

- arithmetic 126
- robust, of low-degree polynomials 111, 112, *see* polynomial, low-degree
- robust, of NC 281
- Chari, S. 89, 231, 270
- Chebyshev’s Inequality *see* Inequality, Chebyshev’s
- Chebyshev’s Theorem *see* Theorem, Chebyshev’s
- Chebyshev, P. 135, 163
- Chen, S. viii
- Cheng, Y. viii
- Chinese Remainder Theorem *see* Theorem, Chinese Remainder
- Chor, B. 300
- Church A. 264
- circuit *see* graph, representing
 - boolean circuit, *see* graph, representing unbounded-fan-in circuit, *see* subcircuit
 - depth reduction *see* reduction, of the depth of a circuit
- circuit family *see* family, circuit
- circuits 175, 197, 200, 276, 279, *see* class, circuit, *see* disjointness, of circuits
 - AND 203, 225
 - AND-OR 88, 201, 206–208, 211, 224, 227, 232
 - bounded-depth 211
 - bounded-fan-in 167, 169–171, 174, 177
 - computing the exclusive-or of three bits via 220
 - constant-depth 207, 212, 213, 218, 223–225, 228, 232
 - constant-depth $2^{\log^{O(1)} n}$ -size 218
 - constant-depth polynomial-size 88, 89, 201, 202, 207, 223, 231, 302
 - constant-depth polynomial-size unbounded-fan-in 280
 - constant-depth subexponential-size 213
 - constant-depth superpolynomial-size 223, 224, 232, 280
 - depth-0 170
 - depth-1 199, 204
 - depth-2 202, 232
 - depth-2 $2^{\log^{O(1)} n}$ -size 89
 - depth-2 $2^{\log^{O(1)} n}$ -size polylogarithmic bottom-fan-in 88, 89
 - depth-2 $2^{\log^{O(1)} n}$ -size probabilistic 88
 - depth-3 $2^{\log^{O(1)} n}$ -size polylogarithmic bottom-fan-in 88
 - depth-4 $2^{\log^{O(1)} n}$ -size polylogarithmic bottom-fan-in 88
 - depth- k 197
 - depth- k bounded-fan-in 174
 - depth- k linear-size 232
 - depth- $\mathcal{O}(k \log k)$ bounded-fan-in 170
 - deterministic 89, 220, 221, 231
 - family of 201
 - for SAT, size of 87
 - for sets in DSPACE[n], size of 87
 - in the shape of a tree 227
 - logarithmic-depth polynomial-size bounded-fan-in 171
 - logspace-uniform 279, 280
 - NC¹ 176
 - OR 205, 210, 225
 - OR-AND 201, 204, 206, 207, 211, 212, 224, 227
 - P-uniform 279
 - parity 260
 - polylog-depth constant-size 308
 - polylog-depth polynomial-size 280, 308
 - polynomial-depth 176
 - polynomial-size 233
 - probabilistic 219, 220, 231
 - small 276, 277
 - small, for BPP 277
 - small, for NP 277
 - small, for the semi-feasible sets 45, 47
 - stratified 198
 - superpolynomial-size 222
 - threshold 260
 - transforming tree into 169
 - unbounded fan-in 198
- class
 - advice *see* advice
 - Arthur–Merlin 300
 - being “almost” closed under an operation 108
 - bounded-ambiguity 43, *see* FewP, *see* UL, *see* UP
 - circuit 88, 279, *see* AC, AC^k, *see* ACC_p, *see* ACC, *see* circuits, *see* NC, NC^k, *see* nonuniform-NC¹, *see* SAC, SAC^k, *see* SC

- counting 64, 82, 290–293, 297, *see* C=L, *see* C=P, *see* PL, *see* PP, *see* #L, *see* #P, *see* SPP
- “exactly-half”-based 192, *see* C=L, *see* C=P
- exponential-time 23, 28, 29, 274, 275, *see* EXP, *see* E, *see* NEXP, *see* NE
- GapP-based characterization of 240
- interactive proof 299, *see* IP, *see* MIP, *see* system, interactive proof
- logspace 82, 277–279, *see* C=L, *see* L, *see* NL, *see* \oplus L, *see* PL
- low-error probabilistic, as intuitively feasible 289
- majority-based 192, *see* PL, *see* PP
- modulo-based 297, *see* coMod_kP , *see* FTM_kP , *see* Mod_kP , *see* ModZ_kP , *see* $\oplus\text{E}$, *see* $\oplus\text{L}$, *see* $\oplus\text{P}$
- modulo-based, logspace analogs 277, *see* $\oplus\text{L}$
- one-way function 31, *see* UP
- optimization-based 297, *see* OptP
- output-cardinality-based 297, *see* SpanP
- polynomial-time 28, 274, *see* P
- probabilistic 277, 290, *see* BPP, *see* PL, *see* PP, *see* RP, *see* ZPP
- “promise”-like 293, *see* BPP, *see* coUP , *see* FewP, *see* RL, *see* RP, *see* UL, *see* UP, *see* ZPP
- query-order-based 303
- uniform complexity 168, *see* advice
- whose name sears the tongues of mere mortals vii
- whose very name contains hundreds of characters vii
- clause 112, 139
- Cleve, R. 27, 194
- clique 165, 166
- closure
 - of a class under a reducibility, potential 235
 - of a class under an operation, potential 235
 - of C=P downward under positive truth-table reductions 260
 - of C=P downward under \leq_{ctt}^p 187, 240, 260
 - of C=P downward under \leq_{dtt}^p 240
 - of C=P downward under \leq_{pos}^p 260, 293
 - of C=P downward under coNP -many-one reductions 241
 - of coC=P downward under \leq_{pos}^p 260, 293
 - of coNP downward under coNP -many-one reductions 241
 - of coNP downward under \leq_{ctt}^p 240
 - of coNP downward under \leq_{dtt}^p 240
 - of \mathcal{F} (a class) under σ (an operation) 92
 - of \mathcal{F} (a class) under integer division 98
 - of LOGCFL under complementation 280
 - of Mod_kP under union 298
 - of natural polynomials under multiplication 247
 - of NP downward under \leq_{pos}^p 268, 307
 - of NP under intersection 268
 - of NP under union 268
 - of OptP under proper subtraction, potential lack of 104, 105
 - of P downward under \leq_{btt}^p 96
 - of P under union 36
 - of $\oplus\text{P}$ downward under \leq_T^p 182
 - of PL downward under P-uniform NC^1 reductions 260
 - of PP downward under constant-round truth-table reductions 249, 251
 - of PP downward under \leq_{btt}^p 245
 - of PP downward under \leq_m^p 239, 245
 - of PP downward under \leq_T^p , potential lack of 252, 259
 - of PP downward under \leq_{tt}^p 235, 245, 293
 - of PP downward under P-uniform NC^1 reductions 260
 - of PP downward under polynomial-time parity reductions 260
 - of PP under complementation 97, 239, 245, 260
 - of PP under disjoint union 245
 - of PP under intersection 235, 242, 244, 245
 - of PP under union 245
 - of probabilistic- NC^1 under intersection 260
 - of P-sel downward under \leq_{pos}^p 296
 - of P-sel under almost-completely degenerate boolean functions 296

- of P-sel under complementation 52, 296
- of P-sel under completely degenerate boolean functions 296
- of P-sel under intersection, lack of 296
- of P-sel under union, lack of 296
- of SAC^k under complementation 280
- of SF_5 downward under \leq_m^p 177
- of #P under addition 76, 87, 92, 100, 101, 106, 287
- of #P under finite sums of multiples of binomial coefficients whose upper element is the input and whose lower element is a constant 107
- of #P under integer division by 2, potential lack of 100, 101, 287
- of #P under integer division, potential lack of 98, 99, 101, 287
- of #P under maximum, potential lack of 100–103, 287
- of #P under minimum, potential lack of 100–103, 287
- of #P under multiplication 92, 93, 101, 106, 287
- of #P under operators in relativized worlds 107
- of #P under proper decrement, potential lack of 100, 105, 106, 287
- of #P under proper subtraction, potential lack of 91, 93, 95, 96, 98, 99, 104, 107, 287
- of SpanP under proper subtraction, potential lack of 105
- of the context free languages downward under \leq_m^p 279
- of Θ_2^p under complementation 20
- of UP under intersection 284
- Cobham, A. 264, 265
- coC=P 260, 293
 - closure properties *see* closure, of coC=P...
- coefficients
 - binomial 93
 - multinomial 93
- cofinite set *see* set, cofinite
- coin
 - fair 74, 131
 - unbiased 288
- collision
 - in image of one-way function 31
- potential relationship between intensity of and collapses 31
- combinatorial game *see* game, combinatorial
- commutativity *see* function, ...commutative...
- of concatenation, lack of 38
- of min 41
- of multiplication 38
- of subtraction, lack of 38
- commutator 168, 172, 174, 175
- coMod_kP 194, 298, 301
- companion
 - best v
- comparison
 - lexicographic *see* order, lexicographic
- complementation
 - closure of LOGCFL under *see* closure, of LOGCFL under complementation
 - closure of PP under *see* closure, of PP under complementation
 - closure of P-sel under *see* closure, of P-sel under complementation
 - closure of SAC^k under *see* closure, of SAC^k under complementation
 - closure of Θ_2^p under *see* closure, of Θ_2^p under complementation
- complete equality *see* equality, complete
- completeness
 - of a protocol 110, 115, 116, 131, 132, 134, 135, 138, 145, 147, 149
 - of a set for a class \mathcal{C} *see* the entry for that class \mathcal{C}
 - of a set for some class \mathcal{C} *see* set, “[that class \mathcal{C}]”-complete
- complexity
 - circuit, of SAT 89
 - Kolmogorov 269
 - nonuniform 45, 51, *see* advice
- complexity theory *see* theory, complexity
- computation
 - ambiguity-bounded 281, 285, *see* FewP, *see* UP
 - bottleneck 181, 300, *see* machine, bottleneck, *see* machine, bounded-width bottleneck, *see* ProbabilisticSSF_k, *see* SF_k, *see* SSF_k
 - deterministic logspace 278, *see* L

- deterministic polynomial-time 22, *see* P
- error-bounded probabilistic 288, 289, *see* BPP, *see* coRP, *see* RP
- exponential-time deterministic 275, *see* EXP, *see* E
- exponential-time nondeterministic 275, *see* NEXP, *see* NE
- majority-based probabilistic symmetric bottleneck 192
- modulo-based 106, 297, 298, *see* coMod_kP , *see* FTM_kP , *see* Mod_kP , *see* ModZ_kP , *see* $\oplus\text{E}$, *see* $\oplus\text{L}$, *see* $\oplus\text{P}$
- nondeterministic logspace 278, *see* NL
- nondeterministic polynomial-time 22, *see* NP
- nondeterministic space-bounded 125, *see* NL
- polynomial-ambiguity 283, *see* FewP
- polynomial-space 176, *see* PSPACE
- PSPACE oracle 213
- quantum 194, 195
- relativized logspace 279
- semi-feasible 294–296, *see* P-sel
- single-valued nondeterministic function 57, *see* NPSV
- unambiguous 281, 283, 285, *see* UL, *see* UP
- unambiguous logspace 84, 85, *see* UL
- zero-error probabilistic 290, *see* ZPP
- concatenation *see* assignments, of concatenation
- condition
 - truth-table 10, 11, 13, 14, *see* refinement, of a truth-table condition
- Condon, A. 164
- coNE 275
- confidence
 - high 109
- configuration
 - unique accepting 126, 129
 - unique middle-point 112
- configuration space *see* problem, robotics configuration space
- conflicting oracle results *see* results, conflicting oracle
- conflicting relativizations *see* results, conflicting oracle
- Conjecture
 - Berman–Hartmanis Isomorphism 26, 282
 - One-Way 282, 285
- coNL 82, 277, 278
- connectivity
 - bidirectional 177
- coNP 5, 6, 28, 52, 59–62, 64, 95–97, 100, 104–106, 194, 240, 241, 269, 271–273, 276, 277, 287, 296, 306, 307, *see* set, coNP-complete, *see* set, potential lack of sparse \leq_m^p -complete, for coNP, *see* set, potential lack of sparse \leq_m^p -hard, for coNP
- closure properties *see* closure, of coNP...
- coNP/linear 52, 296
- coNP/poly 61, 64, 276, 296
- constant function *see* function, constant
- constant-depth circuits *see* circuits, constant-depth, *see* circuits
- constant-to-one function *see* function, constant-to-one
- construction
 - oracle 197, 223
 - widely-spaced 53, 223
- context-free grammar *see* grammar, context-free
- context-free languages
 - closure properties *see* closure, of context-free languages...
- context-free set *see* set, context-free
- Cook’s Theorem *see* Theorem, Cook’s
- Cook, S. 58, 59, 64, 91, 163, 266–268, 275, 279–281, 305, 308
- Cook–Karp–Levin Theorem *see* Theorem, Cook’s
- Cook–Levin Theorem *see* Theorem, Cook’s
- Cormen, T. 266
- coRP 288–290
- coSSF_k 185
- Count 84–86
- counter
 - as auxiliary input 302
- counting
 - enumerative *see* approximation, enumerative
- counting hierarchy *see* hierarchy, counting
- coUP 106, 107, 282, 284
- course, use of this book in *see* textbook, use of this book as

- coUS 284
- Crescenzi, P. 166, 267, 269, 285
- cryptocomplexity
 - average-case *see* cryptography, average-case
 - worst-case *see* cryptography, worst-case
- cryptographic protocol *see* protocol, cryptographic
- cryptography
 - and UP 282, 283
 - average-case 31, 44
 - central role of one-way functions in 31
 - not helped by non-honest functions 32
 - worst-case 31, 33, 44, 282
- Culbertson, E. 270
- culling method *see* method, culling
- cyclic ring *see* ring, cyclic

- DAAD ix
- Damm, C. 87, 277
- DARPA ix
- Davis, M. 264
- Deaett, L. viii
- decision graph *see* graph, decision
- decrementation
 - proper 101
- defeat
 - another element in a tournament *see* tournament, defeat in
 - another element with respect to a P-selector *see* tournament, defeat in
- degree
 - reducibility 240
 - total, of a polynomial 111, 112, 126, 140–144, 147, 148, 150–153, 155, 156, 160, 162
- Demers, A. 269
- DeMillo, R. 163
- Denny-Brown, D. 295
- dense set *see* set, dense
- density 218, 219
- depth
 - of a recursion tree 14
- derandomization 87
- description
 - attribute-value 274
 - instantaneous *see* ID
- determinant
 - of a matrix 148, 149
- deterministic circuits *see* circuits, deterministic
- deterministic machine *see* machine, ...deterministic...
- diagonal elements *see* elements, diagonal
- diagonalization 55, 197, 285
- Díaz, J. 29, 43
- difference
 - symmetric 68, 235, 260
- digital signature protocol *see* protocol, digital signature
- dimension
 - of a matrix 114, 115, 117, 122, 149
- direct product *see* product, direct
- disjoint sets *see* sets, disjoint
- disjoint union *see* union, disjoint
 - closure of PP under *see* closure, of PP under disjoint union
- disjointness 16, 17, 205
 - of intervals 12–14
 - of restrictions 200, 209
 - of subcircuits 205
- disjunctive self-reducibility *see* self-reducibility, disjunctive, of SAT
- disjunctive self-reducible set *see* set, disjunctive self-reducible
- distribution 224, 225
 - probability 219, 299, 302
 - probability, of restrictions 198, 200, 202, 204, 207, 208, 210, 224, 225, 232
 - uniform 116, 131, 162, *see* selection, under uniform distribution
- divide and conquer
 - as a motto 45
- Dolev, D. 193
- domain 32, 33, 37, 38, 44, 121, 122, 141, 142, 152, 247
 - having size at least two 44
 - relation of, between a function and a refinement of that function 58
 - size 84
- double-exponential time *see* time, deterministic double-exponential
- downward closure *see* closure, *see* $R_a^b(C)$, $R_a^b(C)$
- downward path *see* path, downward
- downward separation *see* separation, downward
- DSPACE 87, 89, 271
- DTIME 53, 56, 165, 264, 265, 274, 275, 296
- Du, D. 282

- Durand, A. 108
 Dymond, P. 279, 280
- E 23–25, 28, 64, 265, 268, 273–275,
 307, *see* set, E-complete
 E/linear 64
 $E_a^b(C)$, $E_a^b(C)$ 276, 296, 307
 edge 45, 46, 50–52, 62, 83–86, 177–179,
 198, 199
 Edmonds, J. 264, 265
 element
 – minimum-weight 71
 – range 41, 42
 elements
 – diagonal 82, 159
 elimination
 – Gaussian 146
 Emde Boas, P. van *see* van Emde
 Boas, P.
 Emerson, E. 274
 Encoding
 – Buhrman–Hemaspaandra–Longpré
 28
 – Hartmanis–Immerman–Sewelson
 22, 24, 25, 27, 28
 enumeration
 – of all polynomial-time computable
 functions 216
 – of machines as a central tool in
 proving the existence of complete
 sets 285
 – of NPTMs 58, 268
 – of NPTMs that are unambiguous on
 all inputs, seeming lack of 285
 – of oracle NPTMs clocked in a way
 that holds over all oracles 60
 – of relativized PH machines 213
 – of relativized predicates 221
 – of relativized predicates specifying
 alternating quantifications 221
 enumeration algorithm *see* algorithm,
 enumeration
 enumerative approximation *see*
 approximation, enumerative
 enumerator 119, 163
 – polynomial-time computable 119,
 163, 287, 289
 $E_{k-T}^p(\text{P-sel})$ 296
 $E_{k-itt}^p(\text{P-sel})$ 296
 $E_T^p(\text{P-sel})$ 296
 $E_T^p(\text{SPARSE})$ 276
 equality
 – complete 43
 – weak 43
 Erdős, P. 28
 error
 – one-sided 87, 165, 290
 – two-sided 166
 evaluation
 – query *see* \leq_{tt}^p , *see* reduction,
 polynomial-time truth-table
 evaluator
 – query 247, 248
 evidence
 – relativized 18, 27
 exhaustive search *see* search,
 exhaustive
 EXP 55, 163, 164, 274, 275, 284, 296,
 298, 307, *see* set, EXP-complete
 EXP/linear 296
 expansion
 – of a tree 6
 expectation 135, 137, 203
 exponential hierarchy
 – strong *see* hierarchy, strong
 exponential
 exponential time *see* time, determin-
 istic exponential
 expression
 – arithmetic 138, 140
 factor
 – of approximation 165, 166, 286
 False 1, 3–7, 14, 21
 family
 – circuit 219, 279
 family of circuits *see* circuits, family
 of
 Feige, U. 164–166
 Feigenbaum, J. 64, 163, 164
 Feller, W. 163
 Fellows, M. 284
 Fenner, S. ix, 108, 260, 269, 282, 284,
 290, 293, 294, 298
 FewP 28, 43, 281, 283–285, 287, 293,
 296, 298
 – exponential-time analog of *see*
 analog, exponential-time, of UP,
 FewP, $\oplus\text{P}$, ZPP, RP, or BPP
 Fich, F. 193
 filter 88
 finite monoid *see* monoid, finite
 finite set *see* set, finite
 first 37, 39, 42
 Fischer, D. 289
 Fischer, M. 264, 274, 275, 289
 Fischer, P. 29

- Fischer, S. 287
- flexibility
- of query generation in \leq_T^p 18
- Formula *see* boolean formula
- Lagrange Interpolation 163
 - Newman’s 260
- formula
- 3-CNF 112, 139
 - arithmetic 110
 - boolean 3, 29, 58, 69, 265, 267, 268, 272, 281, 286
 - fully quantified boolean 177
 - quantified boolean 274
 - quantifier-free boolean 274, *see* QBF
 - satisfiable boolean 1, 3–7, 56, 58, 112, 267, 294, *see* SAT
 - unsatisfiable boolean 8, 29
 - variable-free 3, 7
 - well-formed 21
- Forster, J. ix
- Fortnow, L. ix, 28, 108, 163–165, 231, 260, 269, 270, 273, 282, 284, 290, 293, 298
- Fortune, S. 26, 43, 193
- FP 10, 11, 57–59, 64, 78, 80, 81, 89, 119, 236–239, 268, 291, 293, 294, 305–307, *see* function, polynomial-time computable
- Fraenkel, A. 272
- Frankl, P. 28
- Frege proof *see* proof, Frege
- Frost, R. 266
- f_{SAT} 61, 294
- FTM_kP 106, 107, 287
- Fu, B. 260
- function
- ...two-argument... *see* function, ...2-ary...
 - 2-ary 38, 44
 - 2-ary one-way 31, 32, 36, 37, 39, 43
 - 2-ary, definitions of additional properties for 37
 - 2-ary, lower bound on the degree of many-to-one-ness of 44
 - advice 48–50, 52, 67, 82, 84
 - almost-completely degenerate boolean 296
 - almost-completely degenerate boolean, closure of P-sel under *see* closure, of P-sel under almost-completely degenerate boolean functions
 - associative 42, 43, *see* function, ...associative...
 - associative 2-ary 38
 - associative, 2-ary one-way 44
 - associativity of 38
 - boolean 10, 11, 14, 174, 208, 245
 - bounded-ambiguity 35
 - bounded-ambiguity one-way 35, 284
 - census 49
 - characteristic 105, 242
 - characterizing a \leq_{btt}^p -reduction 10
 - commutative 41, 44
 - commutative 2-ary 38
 - commutative, associative, 2-ary 43
 - commutativity of 38
 - completely degenerate boolean 296
 - completely degenerate boolean, closure of P-sel under *see* closure, of P-sel under completely degenerate boolean functions
 - constant 96, 181, 200, 208, 211, 239
 - constant-to-one 35
 - constant-to-one one-way 31, 35
 - determinant 279
 - deterministic 291, 294
 - dishonest 37
 - edge-weight 83
 - gap 235, 236, 258, 260, *see* function, GapP, *see* GapP, *see* GapNC, *see* GapP, *see* $\#gap_N(x)$
 - GapP *see* function, gap, *see* GapP, *see* $\#gap_N(x)$
 - GapP 102, 236, 237, 239–242, 244, 247, 248, 251, 252
 - honest 32–34, 37, 41–43, 269, 282
 - honest 2-ary 37, *see* function, honest
 - honest, strongly noninvertible 43
 - inverse of 32, 34, 35, 37, 42
 - invertible 33
 - k -to-one 35
 - length-decreasing 32
 - low-ambiguity, commutative, associative one-way 42
 - magic 223
 - many-one one-way 268
 - mod 106, 119, 120, 122, 127, 129, 132, 133, 141, 146, 155, 158, 160–162, 193
 - multivalued 56–59, 61, 89, 292, 294

- nondeterministic 56, 291, 294, *see* function, NPMV, *see* NPMV, *see* NPSV
- nondeterministic polynomial-time 56, *see* function, NPMV, *see* NPMV, *see* NPSV
- nondeterministic selector 57
- nondeterministic total 64
- noninvertible 32–34
- NPMV 58, 59, 61, 63–65, 108, 291–294, *see* NPMV
- NPSV 57, *see* NPSV
- NPSV-selector 61–63, 297, *see* NPSV-sel, *see* selectivity
- of a matrix 114
- one-argument one-way 32, 36
- one-to-one 33, 34, 42, 43
- one-to-one one-way 31, 34, 35, 43
- one-way 31–33, 35, 37–39, 42, 43
- optimization 297, *see* function, OptP, *see* OptP
- OptP *see* OptP
- OptP 103–105, 182, 297
- oracle 147, 149, 155
- P-selector 47–49, 51, 54, 297, *see* P-sel, *see* selectivity
- pairing 39, 54, *see* function, standard pairing
- parity 167, 193, 197, 200–202, 204, 206, 207, 213, 216, 218, 219, 222, 224, 231, 232, 280, 297
- partial 38, 43, 57, 59, 61, 62, 64, 282, 291, 294
- partial selector 61
- permanent 110, 112–116, 119, 122
- polynomial-time computability and invertibility of pairing 33
- polynomial-time computable 5, 32, 33, 37, 38, 40, 41, 47, 48, 57, 79, 99, 106, 113, 176, 180, 181, 185, 194, 213–216, 228, 237, 238, 241, 246, 265, 268, 269, 282, 284, 290–292, *see* FP, *see* function, polynomial-time computable...
- polynomial-time computable 2-ary 294, 295
- polynomial-time computable one-to-one 265
- polynomial-time computable total 241
- polynomial-time invertible 32, 33, 41, 246
- polynomial-time invertible 2-ary 37
- polynomial-time noninvertible 37
- polynomial-time selector 295
- polynomial-to-one one-way 43
- polynomially bounded 256
- probabilistic 187
- projection 37
- ranking 286
- recursive 56, 123
- recursive selector 295
- s-honest 37, 38, 41
- s-honest 2-ary 38, *see* function, s-honest
- selector 53, 57, 59, 61, 62, 294, 297, *see* selectivity
- selector, oblivious to the order of its arguments 297
- selector, symmetric 297
- #P 80, 88, 92, 94–97, 99–103, 106, 121, 286, *see* #P
- sign 235, 242
- single-valued 57, 294
- single-valued NPMV *see* NPSV
- special pairing 70
- standard pairing 33, 39–41
- strong, total, commutative, associate one-way 36
- strong, total, commutative, associative 2-ary one-way 36, 37
- strong, total, commutative, associative, 2-ary one-way 40, 42
- strongly noninvertible 2-ary 38
- strongly noninvertible, total, commutative, associative, 2-ary, $\mathcal{O}(n)$ -one one-way 44
- strongly noninvertible, total, commutative, associative, 2-ary, many-one one-way 31, 38, 39, 268
- symmetric 231
- total 236–238
- total single-valued 282
- total, associative, 2-ary one-way 44
- total, associative, 2-ary one-way, upper bounds on the degree of many-to-one-ness of 43
- total, weakly-associative, 2-ary one-way, potential lack of 44
- two-argument... *see* function, ...2-ary...
- unambiguous 35
- unambiguous inversion of 35
- unambiguous one-way 35, 284

- weight 68, 69, 71, 72, 83, 84
- zero, modulo a prime 144
- Füredi, Z. 28
- Fürer, M. 289
- Furst, M. 192, 194, 232, 264, 303

- Gabarró, J. 43
- Gál, A. 87, 89
- gallery
 - rogues’ 263, 305
- Gambosi, G. 166, 267
- game *see* problem, game
 - cat and mouse 264
 - combinatorial 265
 - in a tournament 46
 - of pursuit and evasion 265
- GAP 82, 83, *see* Problem, Graph Accessibility
- $\widehat{\text{GAP}}$ 82–86
- GapL 235, 252–254, 257, 258, *see* function, gap
- GapNC 194, *see* function, gap
- GapP 102, 107, 108, 191, 192, 235–242, 244, 245, 247–249, 251–253, 258–260, *see* function, gap, *see* function, GapP, *see* function, $\#\text{gap}_N(x)$
- Garey, M. 87, 267, 272
- Gasarch, W. ix, 63, 163, 286, 289, 296, 297
- gate
 - AND 88, 89, 172, 177, 178, 198, 201, 217, 229, 279, 308
 - input 172, 174, 198, 217, 229, 230
 - MAJORITY 88, 89
 - MODULO 88, 302
 - OR 88, 89, 172, 173, 176–178, 198, 201, 217, 220, 229, 279, 308
 - oracle 308
 - output 172, 174, 177, 198, 201, 217, 220, 229, 230
 - PARITY 88
 - symmetric 89
 - threshold 232, 260
 - top 198
- Gaussian elimination *see* elimination, Gaussian
- Gavaldà, R. 27, 64, 276
- Geffert, V. ix, 27
- GEM 2, 31, 32, 35, 45, 62, 68, 93, 110, 168, 197, 236
- Gemmell, P. 164
- generator
 - polynomial-time pseudorandom 265
 - pseudorandom 31, 44
 - query 246–248, 251, 257
 - query, length-increasing 246–248, 257
- generators
 - permutation group membership from 264
- Gengler, R. 27
- Gill, J. 87, 106, 231, 232, 260, 268–270, 272, 273, 278, 279, 288–290, 293, 297, 298
- Glaßer, C. 27
- Gödel, K. 264
- Goldberg, A. 265, 286
- Goldreich, O. ix, 269, 289, 300
- Goldschlager, L. 297, 298
- Goldsmith, J. 29, 265, 287, 293, 296
- Goldstein, G. viii
- Goldwasser, S. 163–166, 269, 277, 300
- Goldwurm, M. 286
- Gottlob, G. 269
- Grail
 - Holy 67
- grammar
 - context-free 265, 272
- graph 45
 - automorphism counting in 289
 - decision 193
 - directed, reachability sets in 50
 - representing boolean circuit 279
 - representing unbounded fan-in circuit 198
 - short paths problem in 233
 - topologically sorted directed 278
 - tournament 45, 47, 50, 52, *see* tournament
- Graph Accessibility Problem *see* Problem, Graph Accessibility
- graph isomorphism *see* Problem, Graph Isomorphism
- Graph Isomorphism Problem *see* Problem, Graph Isomorphism
- graphs
 - isomorphic 289
- greedy algorithm *see* algorithm, greedy
- Green, F. viii, 88, 232
- Greenlaw, R. 265
- Grollmann, J. 43, 282–284
- group
 - multiplicative 112

- nilpotent 193
- nonsolvable 167, 174
- nonsolvable permutation 167, 168
- order of *see* order, of a group
- permutation 167, 168
- growth
 - slower, of polynomials 264
- Gruska, J. 194
- guess
 - of an oracle answer 186
- Gundermann, T. 26, 27, 106, 107, 260, 274, 275
- Gupta, S. 88, 106–108, 260
- Gurevich, Y. 269, 283
- Guruswami, V. 166

- Halpern, J. 274
- Han, Y. 27, 265, 277, 289, 295
- hardness *see* NP-hard
 - for UP 283
 - NP 166
 - $\text{NP-}\leq_{btt}^p$ 8, 26
 - $\text{NP-}\leq_{ctt}^p$ 26
 - $\text{NP-}\leq_{dtt}^p$ 26
 - $\text{NP-}\leq_m^p$ 18
 - $\text{NP-}\leq_T^p$ 18, 20
 - of sets, classifying via reductions 305
 - relative, of sets 305
- Hardy, G. 163
- Hartmanis, J. ix, 22, 24, 26–29, 106, 107, 163, 231, 264, 269, 270, 272, 274–277, 282–285, 300
- Hartmanis–Immerman–Sewelson Encoding *see* Encoding, Hartmanis–Immerman–Sewelson
- Hartmanis–Immerman–Sewelson Theorem *see* Encoding, Hartmanis–Immerman–Sewelson
- Håstad, J. 44, 166, 232, 269, 300
- head
 - input-tape 255
 - work-tape 255
- Heberle, E. ix
- Heller, H. 87, 289
- Hemachandra, L. *see* Hemaspaandra, L.
- Hemaspaandra, E. ix, 28, 63, 272–274, 296, 303, 308
- Hemaspaandra, L. iv, ix, 1, 26–29, 43, 44, 63–65, 106–108, 163, 192–194, 231, 260, 265, 268, 269, 272–277, 282–290, 293, 295–298, 303, 308
- Hempel, H. ix, 28, 273, 303
- Hermann, M. 108
- Hertrampf, U. viii, 87, 88, 107, 194, 277, 297, 298, 301, 303
- hierarchy
 - alternation-based, small-space 27
 - arithmetical 270, 271, 277
 - boolean 27
 - bounded to Σ_k^p 28
 - BPP 73, 75
 - C=L 261
 - counting 252
 - counting, logspace analog of 279
 - Kleene 271, 277, *see* hierarchy, arithmetical
 - limited-nondeterminism 29
 - NL 82
 - oracle, of C=L 279
 - oracle, of PL 279
 - PL 252, 254, 256, 260
 - polynomial 1, 18, 22, 25, 28, 29, 43, 50, 56, 58, 63–65, 67, 73, 78, 81, 82, 87, 115, 186, 197, 213, 222, 223, 228, 231, 232, 268–275, 277, 296, 297, *see* Δ_k^p , *see* hierarchy, polynomial, *see* PH, *see* Π_k^p , *see* Σ_k^p , *see* Θ_k^p
 - polynomial, exponential-time analogs of 22, 274
 - polynomial-time *see* enumeration, of relativized PH machines, *see* hierarchy, polynomial
 - probabilistic logspace *see* PLH
 - query, to NP 25, 28
 - strong exponential 22, 27, 275
- Hoang, T. 279
- Hoene, A. 64, 193, 269, 296, 297, 303
- Hoffmann, C. 264
- Hofmann, A. ix
- Holy Grail *see* Grail, Holy
- Holzwarth, F. ix
- Homan, C. viii, 44
- Homer, S. 26, 27, 265, 275, 294
- honest function *see* function, honest
- honesty *see* function, honest
 - why a natural condition 32
- Hoover, H. 265
- Hopcroft, J. 27, 43, 264, 266
- Huang, M. 289, 290
- Hunt, H. 274, 275
- Huynh, D. 272, 286

- ID 255, 256
- Ilardi, P. ix

- Immerman, N. 22, 24, 27–29, 269, 274, 275, 277, 278, 281
 immunity 28, 232, 284
 Impagliazzo, R. 29, 44, 64, 233, 289
 In Polynomial Time We Trust 45
 incantations vii
 Inequality
 – Chebyshev’s 135, 137, 163, 203, 204
 input gate *see* gate, input
 input tape *see* tape, input
 instantaneous description *see* ID
 instantiation
 – random, of variables 110
 integer subtraction *see* subtraction, integer
 interaction 109, 110, 115, 116, 123, 124, 132, 136, 137, 299, *see* system, interactive proof
 interpolation
 – polynomial *see* Technique, Polynomial Interpolation
 interpreter
 – advice 48, 49, 52, 62, *see* advice
 – nondeterministic 51, *see* advice
 – probabilistic *see* advice
 – probabilistic, of advice 49
 intersection
 – closure of NP under *see* closure, of NP under intersection
 – closure of PP under *see* closure, of PP under intersection
 – closure of probabilistic-NC¹ under *see* closure, of probabilistic-NC¹ under intersection
 – closure of UP under *see* closure, of UP under intersection
 interval 12–18, *see* disjointness, of intervals, *see* procedure, interval-pruning, *see* refinement, of a set of intervals, *see* splitting, of intervals
 invariant 4, 5
 inverse
 – matrix 159
 – multiplicative 120, 160
 IP 111, 114, 115, 122, 123, 125, 131, 163, 164, 273, 288, 299, 300, *see* system, interactive proof
 Isolation Lemma *see* Lemma, Isolation
 isomorphism
 – graph *see* Problem, Graph
 Isomorphism
 Istrate, G. viii
 Iwata, S. 264, 265, 272, 274
 Jain, S. 268, 283, 285, 288, 308
 Jenner, B. 278, 289
 Jha, S. 28, 29
 Jiang, Z. 63, 296, 297
 Jockusch, C. 295
 Johnson, D. 87, 267, 272
 Jones, N. 265
 Joseph, D. 282, 283, 296, 297
 JSPS ix
 Jung, H. 260, 278, 279

k-locally self-reducible set *see* set, *k*-locally self-reducible
k-round parallel access *see* access, *k*-round parallel
 Kadin, J. 27
 Kämper, J. 64
 Kann, V. 166, 267
 Kannan, R. 88
 Kannan, S. 27, 164
 Kao, M. 289
 Karloff, H. 163, 270
 Karp, R. 20, 27, 60, 64, 91, 266, 267, 276, 277
 Karp–Lipton Theorem *see* Theorem, Karp–Lipton
 Kasai, T. 264, 265, 272, 274
 Kilian, J. 64, 164, 277, 300
 King Arthur *see* Pendragon, A.
 Kintala, C. 29
 Kleene hierarchy *see* hierarchy, arithmetical
 Kleene, S. 43
 Ko, K. 43, 63, 87, 232, 273, 282, 289, 295, 296, 308
 Kobayashi, K. ix
 Köbler, J. 27, 64, 88, 276, 277, 284, 289, 293, 298, 299
 Koblitz, N. 284
 Kolaitis, P. 108
 Kolmogorov complexity *see* complexity, Kolmogorov
 Kolmogorov-easy string *see* string, Kolmogorov-easy
 Komlós, J. 280
 Kosub, S. ix, 65, 108
 Kozen, D. 266, 272
 Krentel, M. 297
 Ku, J. viii
 Kumar, A. 289
 Kummer, M. 296
 Kunen, K. 265

- Kurtz, S. 108, 260, 269, 275, 282–284, 290, 293, 298
- L 82, 265, 277, 278
- Ladner, R. 265, 268, 274, 279, 308
- Lagakos, D. viii
- Lagrange Interpolation Formula *see* Formula, Lagrange Interpolation
- Landau, H. 64
- Lang, S. 163
- Lange, K. 278
- language *see* set
- canonical complete *see* set, canonical complete
 - leaf 268
- Lapidot, D. 164
- Lasser, W. 265
- Lautemann, C. 194
- leaf 170, 177–180, 198, 199, 217, 227, 230
- leaf language *see* language, leaf
- Learn, A. viii
- Lebesgue measure *see* measure, Lebesgue
- Lee, C. 193, 302
- Leiserson, C. 266
- Lemma
- Isolation 68, 70, 83, 87, 89, *see* Technique, Isolation
 - Switching 207, 232, 233
- length-decreasing function *see* function, length-decreasing
- Levin, L. 44, 64, 91, 164, 165, 267, 268
- Lewin, D. 166
- Lewis, P. 27
- lexicographic comparison *see* order, lexicographic
- lexicographic order *see* order, lexicographic
- lexmin 40, 41
- Li, L. 284
- Li, T. viii
- Lichtenstein, D. 274
- limited-nondeterminism hierarchy *see* hierarchy, limited-nondeterminism
- Lindner, W. 64, 296
- linear-sized advice *see* advice, linear-sized
- Lipton, R. ix, 20, 27, 60, 64, 163, 164, 193, 276, 277
- Liśkiewicz, M. 27
- literals
- conflicting 199
- logarithmic-space boundedness *see* boundedness, logarithmic-space
- LOGCFL 279–281
- closure properties *see* closure, of LOGCFL...
- logic
- branching time 274
 - propositional dynamic 274, 275
- logspace *see* C=L, *see* L, *see* NL, *see* PL, *see* space, logarithmic, *see* UL
- randomized 279
- logspace machine *see* machine, ...logspace...
- logspace reduction *see* reduction, ...logspace...
- logspace-uniform circuits *see* circuits, logspace-uniform
- Long, T. 64, 65, 232, 273, 282, 294, 308
- Longpré, L. 26–28, 308
- Lovász, L. 164–166
- low-degree polynomial *see* polynomial, low-degree
- lower bound *see* bound, lower
- lowness
- of sparse sets 273
- Lozano, A. 27, 277, 298
- Luby, M. 44, 164
- Luks, E. 264
- Lund, C. 163–166, 269, 270
- Lupanov, O. 232
- Lusena, C. 293
- Lynch, N. 279, 308
- MA 164, 275
- Macarie, I. viii
- machine
- alternating 271, 272
 - alternating logarithmic space 280, 281
 - bottleneck 194, 301, 303, *see* computation, bottleneck, *see* ProbabilisticSSF_k, *see* SF_k, *see* SSF_k
 - bounded-width bottleneck 176, 181, 185, 301, 302, *see* computation, bottleneck, *see* ProbabilisticSSF_k, *see* SF_k, *see* SSF_k
 - bounded-width probabilistic symmetric bottleneck 301, *see* ProbabilisticSSF_k
 - bounded-width symmetric bottleneck 185, 186, 301, 302, *see* SSF_k
 - categorical 282, 284, *see* UP
 - deterministic 214

- deterministic logarithmic space 277, 279, *see* L
- deterministic polynomial-space 125, 176, *see* PSPACE
- deterministic polynomial-time 1, 3, 6, 24, 112, 117, 264, 280, 285, 294, 302, 306, *see* P
- deterministic polynomial-time oracle 19, 20, 57, 194, 214, 246, 269
- expected-polynomial-time probabilistic 22, *see* ZPP
- generic 275
- multi-tape 255
- nondeterministic 94, 121, 138, 239, 258, 266, 297, *see* NEXT, *see* NE, *see* NP, *see* tree, computation, of a nondeterministic polynomial-time Turing machine
- nondeterministic exponential-time 23, 24, 112, *see* NEXT, *see* NE
- nondeterministic logarithmic space 82, 277, 278, *see* NL
- nondeterministic logarithmic space oracle 279
- nondeterministic polynomial-time 10, 54, 57–59, 61, 62, 69, 76, 79, 80, 92–106, 113, 139, 182, 183, 186, 238, 239, 251, 260, 266, 281, 283, 285, 286, 290, 291, 294, *see* enumeration, of NPTMs, *see* enumeration, of relativized PH machines, *see* NP
- nondeterministic polynomial-time oracle 19, 20, 76, 80, 186, 213, 269
- nondeterministic polynomial-time, logarithmic space 252, 253
- nondeterministic polynomial-time, logarithmic space oracle 254
- nondeterministic space-bounded oracle 254
- oblivious oracle NL 254, 256
- oblivious RSTNL 256, 257
- polynomial-space 112, 274, *see* PSPACE
- polynomial-time oracle 115
- probabilistic 71, *see* BPP, *see* coRP, *see* PP, *see* RP, *see* ZPP
- probabilistic bounded-width symmetric bottleneck 302, *see* ProbabilisticSSF_k
- probabilistic logarithmic space 278, *see* PL
- probabilistic polynomial-time 49, 70, 75, 138, 288, 290, 291, *see* BPP, *see* PP, *see* RP, *see* ZPP
- probabilistic polynomial-time oracle 72, 75, 110, 134, 138, 142, 299
- probabilistic polynomial-time, logarithmic space 260, *see* PL
- probabilistic symmetric bottleneck 186, 192, 302, 303, *see* ProbabilisticSSF_k
- probabilistic Turing 74, *see* BPP, *see* PP, *see* RP, *see* ZPP
- RSTNL 254, 255
- symmetric bottleneck 185, 194, 302, 303, *see* SSF_k
- symmetric bounded-width bottleneck 185, *see* SSF_k
- unambiguous NP 34, *see* UP
- universal 55
- Maciel, A. ix, 298
- Mahaney’s Theorem *see* Theorem, Mahaney’s
- Mahaney, S. 2, 8, 26, 27, 269, 282, 283
- MAJORITY gate *see* gate, MAJORITY
- MajSat 293
- Marchetti-Spaccamela, A. 166, 267
- Masek, W. 193
- matrix
 - adjacency 82
 - determinant *see* determinant, of a matrix
 - dimension *see* dimension, of a matrix
 - lower triangular 159
 - minor *see* minor, of a matrix
 - nonsingular 149, 278
 - permanent *see* permanent, of a matrix
 - Vandermonde 148, 149, 153
- matrix inverse *see* inverse, matrix
- matrix multiplication *see* multiplication, matrix
- maximally disjoint circuit *see* circuit, maximally disjoint
- maximization 102
- maximum 99–103, 181, 183, 287
 - lexicographic 9, 16
- Mayer, I. ix
- Maynard
 - Brother 67
- McKenzie, P. 194, 260, 289
- measure

- Lebesgue 218
- mechanism
 - acceptance 2
- Meinel, C. 87, 277
- Melkebeek, D. van *see* van Melkebeek, D.
- membership algorithm *see* algorithm, membership
- Merkle, W. ix
- Merlin 300
- method
 - counting 218
 - culling 13, 17
 - isolation 89
 - tableau 112, 127, 139, 163, *see* Theorem, Cook’s
- Meyer, A. 27, 29, 264, 270–272, 275, 277, 296
- Micali, S. 269, 300
- MIN 201, 208–210
- MINIMAL-FORMULAS 272
- minimization 102
- minimum 100–103, 287
 - lexicographic 15
- minimum weight *see* weight, minimum
- minimum-weight element *see* element, minimum-weight
- minimum-weight path *see* path, minimum-weight
- minimum-weight set *see* set, minimum-weight
- minor
 - of a matrix 112, 113, 116, 117, 119, 120
- Minsky, M. 232
- minterm 200, 201, 208, 209
- MinWeight* 68, 69, 84–86
- MinWeightSet* 68, 69
- MIP 111, 133, 134, 137, 138, 164, 165, 275, 299, 300, *see* system, interactive proof
- Mod_kP 87, 194, 297, 298, 301, *see* closure, of $\text{Mod}_k\text{P}\dots$, *see* $\oplus\text{P}$, *see* set, Mod_kP -complete, *see* set, potential lack of sparse \leq_{btt}^P -hard, for Mod_kP
- MODULO gate *see* gate, MODULO
- ModZ_kP 106
- monoid 168, 193, 301
 - aperiodic 193, 301
 - finite 174, 193
 - solvable 193
- monoid operation *see* operation, monoid
- morsel
 - bite-sized 24
- motto
 - of computer science 45
- Motwani, R. 165, 166, 269
- moves
 - randomized, directed by coin tosses 74
- Mukherji, P. viii
- Mulmuley, K. 87, 89
- multilinear polynomial *see* polynomial, multilinear
- multilinear testing *see* testing, multilinear
- multiparty protocol *see* protocol, multiparty
- multiple
 - of a power of 2 79
- multiplication *see* assignments, of multiplication
 - closure of $\#P$ under *see* closure, of $\#P$ under multiplication
- multiplication group *see* group, multiplication
- multiprover protocol *see* protocol, multiprover
- multiset 160
- multivalued function *see* function, multivalued
- multivariate polynomial *see* polynomial, multivariate
- Mundhenk, M. 27, 277, 293
- Naik, A. 29, 63–65, 88, 265, 276, 284, 295–297
- Nasipak, C. 63
- Nasser, N. 260
- natural polynomial *see* closure, of natural polynomials under multiplication, *see* polynomial, natural
- NC, NC^k 167, 168, 171, 174, 176, 193, 195, 260, 261, 269, 279–281, 293, 301, 302, 308, *see* characterization, robust, of NC, *see* class, circuit
- NC^1 circuits *see* circuits, NC^1
- NE 23–25, 28, 265, 268, 274, 275, *see* set, NE-complete
- near-testable set *see* set, near-testable
- nearly near-testable set *see* set, nearly near-testable

- Neumann, J. von *see* von Neumann, J.
- Newman's Formula *see* Formula, Newman's
- Newman, D. 260
- NEXP 110, 112, 133, 134, 137, 138, 145, 163–165, 274, 275, 300
- NIA ix
- Nickelsen, A. 297
- nilpotent group *see* group, nilpotent
- Nisan, N. 28, 163, 164, 270, 278, 279
- NL 67, 68, 82–84, 87, 89, 277, 278, 280, 281, *see* set, NL-complete, with respect to 1-L reductions, *see* set, NL-complete
- NL hierarchy *see* hierarchy, NL
- NL/poly 68, 82, 84, 278
- nonapproximability *see* approximation
- of NP optimization problems 166, 267
- nonconstructive proof *see* proof, nonconstructive
- nondeterminism 20, 267, *see* FewP, *see* NEXP, *see* NE, *see* NL, *see* NP, *see* UL, *see* UP
- ambiguous 87
- linear 52
- unambiguous 87
- nondeterministic algorithm *see* algorithm, nondeterministic
- nondeterministic auxiliary push-down automata *see* automata, nondeterministic auxiliary pushdown
- nondeterministic machine *see* machine, ...nondeterministic...
- noninvertibility
- of non-honest functions 32
- strong 37–39, 41, 43
- noninvertible function *see* function, ...noninvertible...
- nonleaf *see* leaf
- nonsingular matrix *see* matrix, nonsingular
- nonsolvable group *see* group, nonsolvable
- nonuniform complexity *see* complexity, nonuniform
- nonuniform deterministic finite automata *see* NUDFA
- nonuniform-NC¹ 167, 168, 171, 174
- normalization
- of coin tosses 74
- Notes
- Bibliographic ix, 26, 38, 43, 63, 64, 87, 106, 163, 192, 231, 260, 308
- NP 1–3, 5, 6, 8–11, 18–29, 31, 33–35, 39, 41, 43–45, 49–65, 67–70, 72, 73, 87, 89, 91, 93–100, 102, 104–106, 109, 131, 163–166, 185, 186, 192, 194, 197, 231, 232, 263–278, 282–287, 289, 292–294, 296–301, 305–308, *see* circuits, small for NP, *see* machine, nondeterministic polynomial-time, *see* SAT, *see* set, NP-complete ones that are non-isomorphic, *see* set, NP-complete, ones that are P-isomorphic, *see* set, NP-complete, relativizably so, *see* set, NP-complete, *see* set, possibility of NP having sparse Turing-complete, *see* set, possibility of NP having sparse Turing-hard, *see* set, potential lack of sparse \leq_{btt}^p -hard, for NP, *see* set, potential lack of sparse \leq_{dt}^p -hard, for NP, *see* set, potential lack of sparse \leq_m^p -complete, for NP, *see* set, potential lack of sparse \leq_T^p -complete, for NP, *see* set, potential lack of sparse \leq_T^p -hard, for NP, *see* set, potential lack of tally \leq_m^p -complete, for NP, *see* set, potential lack of tally \leq_m^p -hard, for NP, *see* set, sparse, in NP, *see* set, sparse, in P, *see* tree, computation, of a nondeterministic polynomial-time Turing machine
- closure properties *see* closure, of NP...
- NP-hard 3, 6, 8, 9, 11, 19–22, 26, 27, 29, 60, 268, 296, *see* hardness, NP...
- NP-hardness *see* hardness, NP..., *see* NP-hard
- NP-hardness of approximation *see* approximation, NP-hardness of
- NP-printable set *see* set, NP-printable
- NP-selective set *see* set, NP-selective
- NP/linear 49, 51, 52, 63, 296
- NP/poly 61, 64, 276, 296
- NPFewV 65
- (NP \cap coNP)/poly 59–62, 64, 276, 296
- NPkV 65
- NPMV 57–59, 61, 63–65, 89, 108, 291–294, 306, *see* function, NPMV
- NPSV 57–59, 61–65, 291–295, 297, *see* refinement, NPSV

- NPSV-sel 59, 61, 62, 296, *see* function, NPSV-selector
- NPTM *see* machine, nondeterministic polynomial-time
- NSF ix
- NTIME 266, 267, 274, 275
- NUDFA 193, 301
- number
 - of primes 122
- oblivious machine *see* machine, oblivious...
- obliviousness
 - of selector functions 297
- Ogihara, Ellen ix
- Ogihara, Emi ix
- Ogihara, Erica ix
- Ogihara, M. iv, ix, 1, 26, 27, 29, 63–65, 87, 106–108, 193, 194, 260, 261, 265, 269, 276–279, 287, 290, 293–298, 301, 303, 308
- Ogihara–Watanabe Theorem *see* Theorem, Ogihara–Watanabe
- Ogiwara, M. *see* Ogihara, M.
- one-sided error *see* error, one-sided
- One-Way Conjecture *see* Conjecture, One-Way
- one-way function *see* function, ...one-way...
- operation 92, 99, 107
 - 1-ary 100
 - 2-ary 100
 - associative 168, 169
 - boolean 280
 - monoid 169
 - multi-argument 107
 - one-argument 107
 - polynomial-time computable 92, 93, 95–99, 101, 104, 105, 108, 287
- operator
 - BP 87, 88, 301
 - R 87, 88, 297
- optimal advice *see* advice, optimal
- optimization function *see* function, optimization
- optimization problem *see* problem, NP optimization
- OptP 103–105, 107, 108, 181–183, 297, 299, *see* function, OptP
 - closure properties *see* closure, of OptP...
- OR circuits *see* circuits, OR
- OR gate *see* gate, OR
- OR-AND circuits *see* circuits, OR-AND
- oracle 19–21, 28, 29, 57, 64, 72, 75, 81, 87, 107, 115, 121, 123, 132, 134–138, 141, 142, 144, 146, 147, 149, 151, 152, 155, 163–165, 187, 192, 197, 207, 213, 214, 216, 218, 222, 223, 228, 231, 246, 247, 249–252, 254–258, 268–270, 282, 284, 285, 293, 306, 308, *see* separation, by an oracle, *see* world, relativized
 - C=P 192
 - \oplus P 76
 - PSPACE-complete 197
 - #P 80
 - NP 1, 19, 89
 - perm 115–117
 - PH 194
 - PL 256
 - random 64, 89, 219, 232, 268, 269, 273, 282, 300
 - sparse 21
- oracle construction *see* construction, oracle
- oracle function *see* function, oracle
- oracle gate *see* gate, oracle
- oracle machine *see* machine, ...oracle...
- order
 - among the variables 199, 200
 - lexicographic 5, 7, 9, 12, 14–16, 36, 40, 42, 55–57, 80, 91, 100, 101, 163, 194, 228, 238, 265
 - of a group 112
 - of all possible moves 138
 - of instructions 181, 185
 - of the nodes in a graph 82
 - of the non-appendix chapters viii
- Othello 272
- overhead
 - quadratic 55
- P 1, 2, 5, 8–12, 18, 19, 22–29, 33–36, 39–41, 43, 44, 47–49, 57, 60, 63, 68, 70, 72–78, 80–82, 87, 91, 93, 95, 97–99, 106, 107, 110, 112, 114, 115, 119, 139, 163–165, 183, 187, 194, 197, 231, 232, 236, 240, 252, 259, 263–277, 282–287, 289, 293–298, 300, 305, 306, 308, *see* machine, deterministic polynomial-time, *see* set, potential lack of sparse \leq_{btt}^p -hard, for P
- P-capturable set *see* set, P-capturable
- P-close set *see* set, P-close

- P-immune *see* immunity
- P-immunity *see* immunity
- P-isomorphism 26, 31, 269, 278, 282
- P-sel 47–49, 51, 52, 56, 63, 64, 276, 294–296, 298, *see* circuits, small, for the semi-feasible sets, *see* function, P-selector
 - closure properties *see* closure, of P-sel...
- P-selector function *see* function, P-selector
- P-uniform circuits *see* circuits, P-uniform
- P-uniformAC¹(C=P) 293
- P-uniformAC^k(C=P) 308
- P-uniformNC¹(C=P) 293
- P-uniformNC^k(C=P) 308
- P/linear 48, 63
- P/poly 22, 27, 47, 48, 60, 63, 75, 76, 78, 87, 164, 263, 275–277, 289, 296
- P/quadratic 48, 49, 63, 276, 296
- padding *see* set, paddable, *see* set, padded version of, *see* translation, via padding
 - of strings 49
- pair
 - matrix-integer 115, 117
- pairing function *see* function, pairing, *see* function, standard pairing
- Papadimitriou, C. ix, 87, 271, 272, 274, 275, 297, 298
- Papathanasiou, T. ix
- Papert, S. 232
- parallel access to NP *see* access, parallel, to NP
- parallel queries *see* queries, parallel
- parameterized strategy *see* strategy, parameterized
- Parberry, I. 297, 298
- parity
 - of #acc 76, 77
 - of a number 239
- parity circuits *see* approximation, of threshold circuits by parity circuits, *see* circuits, parity
- parity exponential time *see* time, parity exponential
- parity function *see* function, parity
- PARITY gate *see* gate, PARITY
- Parkins, K. 63
- partial function *see* function, partial
- partition
 - of potential queries 216, 222, 229
 - of variables 224
- Pasanen, K. 43
- Paterson, M. 296
- path *see* reduction, of the number of accepting paths
 - downward 174, 177, 179, 198
 - minimum-weight 83, 84, 86
 - nondeterministic 62, *see* machine, nondeterministic polynomial
 - rejecting computation 59, 99, 101, 105, 235, 236, 238, 294, *see* #rej_N(x)
 - unique accepting computation 281, 285
 - unique minimum-weight 84
 - unique successful computation 86
- paths
 - shortness of, in a tournament 51
- Paturi, R. 260
- Paul, W. 193
- PBP 167, 168, 171, 174, 193, 300–302
 - width of *see* width, of PBP
- P^{C=P} *see* set, P^{C=P}-complete
- PCP Theorem *see* Theorem, PCP
- PCP(*f*(*n*), *g*(*n*)) 165, 269
- pebble 167, 232
- pebbling game *see* game, pebbling
- Pendragon, A. 67, 300
- perceptron 232
- perm 113–122, *see* permanent
- permanent *see* perm, *see* protocol, for permanent
 - of a matrix 112, 113, 115, 118, 119
- permanent function *see* function, permanent
- permutation 113, 114, 121, 172, 185, 188–190, 192, 193, 302
- permutation group *see* group, permutation
- permutation group membership *see* generators, permutation group membership from
- PH 19, 20, 22, 27, 43, 58, 60, 61, 64, 67, 68, 73, 78, 81, 82, 87, 88, 97, 101, 105, 115, 119, 164, 194, 197, 207, 213, 218, 219, 221–223, 228, 231, 232, 259, 271–273, 276, 286, 287, 289, 293, 294, 297, 298, 301, *see* hierarchy, polynomial, *see* set, sparse, in PH
 - exponential-time analog of *see* analog, exponential-time, of the polynomial hierarchy
- Pinheiro, E. ix
- Pippenger, N. 279–281

- Pitassi, T. 232, 233
- PL 82, 252, 254, 256, 260, 278–280, *see* set, canonical complete for PL, *see* set, PL-complete
- closure properties *see* closure, of PL...
- PL hierarchy *see* hierarchy, PL
- PL oracle hierarchy *see* hierarchy, oracle, of PL
- PLH 254
- $P^{NP[\mathcal{O}(\log n)]}$ 1, 19, *see* Θ_k^P
- polylog-depth circuits *see* circuits, polylog-depth constant-size, *see* circuits, polylog-depth polynomial-size
- polynomial *see* specification, unique, of a polynomial by coefficients, *see* specification, unique, of a polynomial by points, *see* specification, unique, of a polynomial
- increasing 75
 - low-degree 111, 112, 242, *see* characterization, robust, of low-degree polynomials
 - multilinear 141, 164
 - multivariate 111, 112, 141, 156, 235
 - natural 247, 248, 251, 255–257
 - nonzero 111, 112, 150, 151
 - root of *see* root, of a polynomial
 - strictly increasing 11, 75, 184, 247
 - two-variable 242
 - univariate 111
- polynomial hierarchy *see* hierarchy, polynomial
- polynomial interpolation *see* Technique, Polynomial Interpolation
- polynomial machine *see* machine, ...polynomial...
- polynomial-depth circuits *see* circuits, polynomial-depth
- polynomial-size circuits *see* circuits, polynomial-size
- polynomial-space boundedness *see* boundedness, polynomial-space
- polynomial-time algorithm *see* algorithm, polynomial-time
- polynomial-time boundedness *see* boundedness, polynomial-time
- polynomial-time computable enumerator *see* enumerator, polynomial-time computable
- polynomial-time computable function *see* function, polynomial-time computable
- polynomial-time computable operator *see* operator, polynomial-time computable
- polynomial-time predicate *see* predicate, polynomial-time
- polynomial-time reduction *see* reduction, ...polynomial-time...
- polynomial-time relation *see* relation, polynomial-time
- Pomerance, C. 277
- position
- input-tape head 255
 - work-tape head 255
- Post, E. 264
- power
- relative, of different complexity classes 22
- PP 49, 50, 67, 68, 78, 80–82, 87, 94–99, 101, 105–107, 112, 119, 186, 232, 235–237, 239–242, 244, 245, 247–252, 259, 260, 263, 273, 279, 286, 287, 290–293, 296–298, 300, 301, *see* class, counting, *see* set, PP-complete
- closure properties *see* closure, of PP...
- PP/linear 49, 50
- P^{PP} *see* set, canonical complete for P^{PP}
- Pr 135, 187–189, 191, 208–210, 278, 288, 291, 302
- Pratt, V. 163, 274
- predecessor 180, 194
- predicate
- polynomial-time 95, 102, 103, 267, 271, 283, 288, 292, 298
- preimage 34, 42
- primality *see* certificate, of primality, *see* number, of primes, *see* set, of all prime numbers, *see* set, of primes
- complexity of 99, 267, 277, 284, 289, 290
 - complexity of certificate checking 131, 132, 142
- Prime Number Theorem *see* Theorem, Prime Number
- Principle
- Pigeonhole 222, 233
- probabilistic circuits *see* circuits, probabilistic

- probabilistic function *see* function, probabilistic
- probabilistic logspace hierarchy *see* PLH
- probabilistic machine *see* machine, ...probabilistic...
- probabilistic oracle protocol *see* protocol, probabilistic oracle
 - NC^1
 - closure properties *see* closure, of probabilistic- NC^1 ...
- probabilistic- NC^1 260
- Probabilistic-PSPACE 273
- probabilistically checkable proof *see* proof, probabilistically checkable
- ProbabilisticSSF_k 186, 188, 192, 301, 302
- probability
 - acceptance 116, 117, 123, 124, 134–136, 289
 - maximum acceptance 116, 124
- probability distribution *see* distribution, probability
- Problem
 - Graph Accessibility 82, 89, *see* GAP
 - Graph Isomorphism 267, 269, 289
 - Unique Optimal Traveling Salesperson 272
- problem *see* set
 - NP optimization 166, 266, 267
 - adversary 274
 - boolean formula minimization 272
 - canonical complete *see* set, canonical complete
 - evaluation, of polynomials over integer matrices 278
 - game 274
 - game-based 274
 - pebbling 264
 - PSPACE 124
 - robotics configuration space 264
 - word 193
- procedure
 - enumeration 12, 13
 - interval-pruning 1, 12–18
 - nondeterministic logarithmic space 84, *see* NL
 - polynomial-time 12, 13, *see* FP, *see* P
 - polynomial-time search 12
 - self-reducibility-based tree-pruning 2
 - tree-pruning 1–3, 6
- product
 - direct 193
 - of all prime divisors 298
 - partial 175
- program
 - bounded-width branching 167, 168, 193, 194, 300–302
 - bounded-width-branching *see* PBP
 - branching 172, 193, *see* PBP
 - branching, generalizing the notion 174
 - over a monoid 193
 - straight-line 164, 194
- programs *see* machine, *see* PBP, *see* procedure
 - bounded-width permutation-only branching 194
 - bounded-width polynomial-size branching 168, 169, 172, 173, 301
 - polynomial-size, permutation-only branching 193
- projection function *see* function, projection
- promise
 - in the definition of SPP 290
 - in the definition of UP 285
- proof
 - census-based 20
 - deterministically verifiable 109
 - Frege 233
 - nonconstructive 198
 - probabilistically checkable 267, *see* PCP($f(n), g(n)$)
 - relativizable 60
- proper decrement *see* decrement, proper
- proper subtraction *see* subtraction, proper
- property *see* closure
 - \leq_T^p -hardness, of PP for PH 50, 67
 - closure, hardest 93
 - closure, of $C=L$ 261
 - closure, of #P 94, 98, 99
 - closure, of #P involving binomial and multinomial coefficients 93
 - intermediate closure 99
 - NP-completeness, of SAT under \leq_m^p -reduction 61
 - one-argument, of GapP 108
 - one-to-one, of one-way functions 34, 44

- polynomial-time computable closure 107
- polynomial-time computable closure, of OptP 104
- propositional dynamic logic *see* logic, propositional dynamic
- Protasi, M. 166, 267
- protocol 110, 112, 115–119, 123, 125, 126, 129, 131, 136, 147–149, 153, 165, *see* completeness, of a protocol, *see* interactive protocol, *see* soundness, of a protocol, *see* system, interactive proof
 - building block for 31, 36, 43
 - cryptographic 31, 36
 - digital signature 43
 - for an interactive proof system 109
 - for permanent 110, 115, 116
 - for PSPACE 132
 - for reachability 126
 - fully parallelized multiprover interactive proof 164
 - multiparty 36
 - multiprover 164
 - one-round perfect-zero-knowledge 164
 - one-sided-error PCP 166
 - probabilistic oracle 134, 135, 138, 142, 164, 165
 - probabilistic polynomial-time protocol 269
 - two-prover 135
 - two-sided-error PCP 166
- prover 109–111, 115, 116, 118, 119, 123–125, 131–136, 163, 165, 299, 300, *see* system, interactive proof
 - deterministic 123, 134, 136
 - power of 109
- pruning
 - tree 5, 6
- pseudorandom generator *see* generator
- PSPACE 22, 23, 87, 110, 112, 122, 124–126, 133, 163, 164, 176, 177, 181, 194, 197, 207, 213, 218, 219, 222, 231, 232, 263, 270–275, 285, 287, 293, 300, 301, 303, *see* protocol, for PSPACE, *see* QBF, *see* set, PSPACE-complete, *see* tree, computation, of a deterministic polynomial-space Turing machine
- pushdown automata *see* automata, pushdown
- Python, M. 67
- QBF 176, 177, 181, 274, *see* PSPACE
- quadratic bound *see* bound, quadratic
- quantified boolean formula *see* formula, quantified boolean
- quantifier
 - block, existential or universal 272
- quantifier switching *see* switching, quantifier
- quantifiers
 - alternating 221, 271, 272, 274
- quaternary tree
 - full *see* tree, full quaternary
- qubit 194, 195
- queries
 - parallel 250
- query generator *see* generator, query
- query round *see* round, query
- query simulation algorithm *see* algorithm, query simulation
- query state *see* state, query
- query tape *see* tape, query
- Rabi, M. 36, 43, 44
- Rabin, M. 264, 277
- Rackoff, C. 87, 279, 284, 300
- Ramachandran, A. 29, 231, 269
- random bits *see* bits
- random oracle *see* oracle, random
- random restriction *see* restriction, random
- random self-reducibility *see* self-reducibility, random
- random variable *see* variable, random
- randomized algorithm *see* algorithm, randomized
- randomized moves *see* moves, randomized, directed by coin tosses
- randomness 67, 109, 110, 186, 299
- range 32, 34, 35, 37, 38, 282, 284, 286
- Ranjan, D. 231, 270, 300
- rank
 - of a string 80, 114, 169, 181–185, 187, 188, 191, 236, 238
- rankable set *see* set, rankable
- ranking function *see* function, ranking
- Rao, R. 28
- $R_a^b(C)$, $R_a^b(C)$ 18, 19, 22, 27, 60, 64, 269, 271, 273, 293, 296, 298, 307, 308
- Reach 84–86
- reachability 50, 51, 82, 84, 112, 129, *see* protocol, for reachability
- ReachTest 85, 86

- recurrence relation *see* relation, recurrence
- recursion
 - bounded depth of *see* bounded, depth of recursion
- recursive call *see* call, recursive
- recursive function *see* function, recursive
- recursive set *see* set, recursive
- reducibility closure *see* $R_a^b(C)$, $R_a^b(C)$
- reduction
 - \leq_m^p , of languages in SSF_k 301
 - 1-L 278
 - as a means for studying relative hardness of sets 305
 - between functions 121
 - coNP-many-one 241, 306, 308, *see* \leq_m^{conp}
 - coNP-many-one, closure of $\text{coC}=\text{P}$ downward under *see* closure, of $\text{coC}=\text{P}$ downward under coNP-many-one reductions
 - coNP-many-one, closure of coNP downward under *see* closure, of coNP downward under coNP-many-one reductions
 - constant-round truth-table, closure of PP downward under *see* closure, of PP under constant-round truth-table reductions
 - Cook’s 305, 308
 - logspace bounded-truth-table 265
 - logspace many-one 306, *see* \leq_m^L
 - logspace-uniform AC^k 308
 - logspace-uniform NC^k 308
 - NC^1 many-one 308
 - of error-probability in BPP computation 73
 - of numbers of solutions 108
 - of numbers of witnesses 108
 - of the cardinality of a set of vectors 88
 - of the cardinality of acceptance types 108
 - of the depth of a circuit 206
 - of the number of accepting paths 94
 - of the number of outputs 292
 - of the number of solutions 65, 67
 - one-way logspace 278
 - P-uniform AC^k 308
 - P-uniform NC^1 , closure of PL downward under *see* closure, of PL downward under P-uniform NC^1 reductions
 - P-uniform NC^1 , closure of PP downward under *see* closure, of PP downward under P-uniform NC^1 reductions
 - P-uniform NC^k 308
 - polynomial-time bounded-truth-table 2, 9, 18, 26, 96, 245, 306, *see* \leq_{btt}^p
 - polynomial-time conjunctive truth-table 240, 241, 305, *see* \leq_{ctt}^p
 - polynomial-time conjunctive Turing 306, *see* \leq_c^p
 - polynomial-time conjunctive-truth-table 26
 - polynomial-time constant-round truth-table 240, 249–251, *see* $\leq_{\text{tt}[k]}^p$
 - polynomial-time disjunctive truth-table 240, 305, *see* \leq_{dtt}^p
 - polynomial-time disjunctive Turing 306, *see* \leq_d^p
 - polynomial-time disjunctive-truth-table 26
 - polynomial-time locally positive Turing 306, *see* \leq_{locpos}^p
 - polynomial-time many-one 3, 6, 8, 9, 61, 71, 305, *see* \leq_m^p
 - polynomial-time parity, closure of PP downward under *see* closure, of PP downward under polynomial-time parity reductions
 - polynomial-time positive Turing 306, *see* \leq_{pos}^p
 - polynomial-time randomized *see* $\leq_{\text{randomized}}$
 - polynomial-time truth-table 246–248, 305, *see* \leq_{tt}^p
 - polynomial-time Turing 18, 259, 305, *see* \leq_T^p
 - polynomial-time two-round truth-table 250, 251, *see* $\leq_{\text{tt}[k]}^p$
 - positive truth-table, closure of $\text{C}=\text{P}$ downward under *see* closure, of $\text{C}=\text{P}$ under positive truth-table reductions
 - randomized 67, 69, 70
 - randomized, of NP-language to USAT 70
 - strong nondeterministic *see* \leq_T^{sn}
 - witness 93–95, 106, 108
- refinement
 - $\text{FP}_{\text{tt}}^{\text{NP}}$ 64, 89
 - $\text{FP}_{\text{UP}}^{\text{UP}}$ 293

- NPFewV 65
- NP k V 65
- NPSV 58, 59, 61, 63, 65, 292–294
- of a multivalued function 58, 64, 292, 294
- of a set of intervals 12–17
- of a truth-table condition 14
- Regan, K. viii, 87, 88, 106, 285
- Reingold, N. 89, 260
- Reinhardt, K. 89
- Reischuk, R. 27
- Reith, S. 277
- rejecting computation path *see* path, rejecting computation
- rejection cardinality *see* cardinality, rejection
- relation
 - polynomial-time 266, 287
 - recurrence 47
 - relativizable 213, 260
- relativizable result *see* result, relativizable
- relativization 60, 73, 78, 231
 - by sparse oracles 273
 - RST *see* relativization, Ruzzo–Simon–Tomp
 - Ruzzo–Simon–Tomp 82, 254, 260, 268–270, 279
- relativizations, conflicting *see* results, conflicting oracle
- relativized world *see* world, relativized
- replacement
 - of provers with an oracle 134
 - of the oracle 75
- research
 - esoteric vii
- restriction 198–200, 202, 204, 206–212, 224, 225, 227, 228, *see* disjointness, of restrictions, *see* distribution, probability, of restrictions
 - disjoint pair 200
 - empty 200
 - product 200, 224
 - random 202, 204, 224, 225
 - size of 200
- result
 - partial 100, 107
 - relativizable 60, 72, 73, 75
- results
 - conflicting oracle 87, 197, 270
- Rettinger, R. ix, 27
- reversal
 - of the accepting and rejecting path behavior 100
- Rice’s Theorem *see* Theorem, Rice’s
- Rice, H. 285
- ring
 - cyclic 193
 - zero-divisor of *see* zero-divisor, of a ring
- Rivest, R. 36, 43, 266
- RL 279
- Roche, J. ix
- Rochester ix
 - University of viii
- Rogers, H., Jr. 271
- Rogers, J. 65, 282, 284
- Rohatgi, P. 89, 231, 270
- Rompel, J. 163
- root
 - of a polynomial 111–113, 150, 151, 207, 208, 211
 - of a tree 5, 7, 92, 180
- Rossmanith, P. 278
- Rothe, J. ix, 28, 43, 44, 63, 272, 284, 285, 287, 297
- round
 - of the integer sampling algorithm 131
 - parallel query 251
 - query 249–252
 - simulation 136, 137
- Royer, J. 65, 269, 275, 282–284
- Rozenberg, G. ix
- RP 28, 29, 72, 87, 268, 288–290, 296
 - exponential-time analog of *see* analog, exponential-time, of UP, FewP, \oplus P, ZPP, RP, or BPP
- RP operator *see* operator, RP
- $R_{btt}^p(\text{NP})$ 307
- $R_{btt}^p(\text{P-sel})$ 296, 298
- $R_{cct}^p(\text{SPARSE})$ 307, 308
- $R_{cct}^p(\text{TALLY})$ 307, 308
- $R_{k-T}^p(\text{NP})$ 269
- $R_{k-T}^p(\text{P-sel})$ 296
- $R_{k-T}^p(\Sigma_i^p)$ 273
- $R_{k-tt}^p(\text{NP})$ 269
- $R_{k-tt}^p(\text{P-sel})$ 296
- $R_{\mathcal{O}(\log n)-T}^p(\text{NP})$ 271, 273
- $R_{\mathcal{O}(\log n)-T}^p(\Sigma_k^p)$ 271
- $R_{\mathcal{O}(n)-T}^p(\text{P-sel})$ 64
- $R_{pos}^p(\text{NP})$ 307
- $R_T^p(\text{SPARSE})$ 22, 27
- $R_{tt}^p(\text{C=P})$ 260, 293
- $R_{tt}^p(\text{NP})$ 18, 19

- Rubinfeld, R. 163, 164, 284
 Rubinstein, R. 43, 283–285
 Rudich, S. 265, 286
 Rumely, R. 277
 runtime 19, 20, 24, 34, 76, 80, 123, 124, 138, 183, 186–188, 214, 236, 256
 Russell, A. 27, 164
 Russo, D. 260
 Ruzzo, W. 82, 254, 260, 265, 279–281
- s-honest function *see* function, s-honest
 Sabadini, N. 286
 SAC, SAC^k 279–281, *see* class, circuit
 – closure properties *see* closure, of SAC^k ...
 safe storage *see* storage, safe
 Safra, S. 164–166
 Saks, M. 260
 Salomaa, A. ix
 Samorodnitsky, A. ix, 166
 sampling algorithm *see* algorithm, sampling
 Santha, M. 279
 SAT 1, 3–9, 19–22, 26, 57–61, 87, 89, 91, 93, 95, 98, 267–270, 273, 276, 282, 284, 287, 289, 296, 305, *see* circuits, for SAT, size of, *see* NP
 satisfiable formula *see* formula, satisfiable boolean
 satisfying assignment *see* assignment, satisfying, *see* assignments
 Savage, J. 276
 Savitch's Theorem *see* Theorem, Savitch's
 Savitch, W. 89, 125, 163, 273
 Saxe, J. 232
 SC 279
 Schaefer, M. ix, 272
 Schaefer, T. 272
 Schear, M. ix
 scheme
 – oracle construction 213, 215
 – pruning 5
 Scherer, B. viii
 Schöning, U. ix, 27, 87, 269, 273, 276, 277, 284, 286, 287, 289, 293, 296, 298, 299
 Schulman, L. 194
 Schwartz, J. 163, 264
 Schwentick, T. 88, 194
 Scully, V. 263
 search
 – brute-force 53, 54
 – exhaustive 264
 search procedure *see* procedure, polynomial-time search
second 37, 39, 42
 secret
 – of complexity theory vii
 – real, of complexity theory vii
 secret-key agreement *see* agreement, secret-key
 Seiferas, J. viii, ix, 275, 279
 selection
 – random, of an oracle 218
 – under uniform distribution 71, 80, 81, 116, 118, 131–133, 146, 154, 160–162, 187, *see* distribution, uniform
 selectivity 62, 64, *see* function, NPSV-selector, *see* function, P-selector, *see* function, P-sel, *see* function, selector, oblivious to the order of its argument, *see* function, selector, symmetric, *see* function, selector, *see* NPSV-sel, *see* P-sel, *see* set, semi-feasible-sel
 – counting-class-based 64
 – importance of 295
 – nondeterministic and other analogs of P-selectivity 64
 selector function *see* function, selector
 self-correction 164
 self-reducibility 4, 5, 60, 119
 – disjunctive *see* tree, disjunctive self-reducibility
 – disjunctive, of SAT 1
 – downward 164
 – many-one 194
 – of SAT 2
 – random 164
 – tree *see* tree, self-reducibility
 self-reducibility algorithm *see* algorithm, self-reducibility
 self-reducibility-based argument *see* argument, self-reducibility-based
 self-reducibility-based tree-pruning approach *see* approach, self-reducibility-based true-pruning
 self-testing 164
 Selman, A. viii, ix, 43, 44, 63–65, 268, 273, 276, 282–284, 294–297, 308
 semi-feasible set *see* set, semi-feasible
 semi-membership algorithm *see* algorithm, semi-membership

- semi-recursive set *see* set, semi-recursive
- Sengupta, S. ix, 27, 164
- separation
 - by an oracle 231, 232, 259, 272, 273, 284, 293, 297, 298, *see* oracle
 - downward 273
 - probability one 284, 300
- set
 - 2-disjunctively self-reducible 60
 - almost polynomial-time 296
 - $C=L$ -complete 278
 - $C=P$ -complete 293
 - canonical complete for PL 278
 - canonical complete for P^{PP} 293
 - cofinite 219
 - complete for the \leq_{tt}^L -reducibility closure of $C=L$ 279
 - complete, for levels of PH 272
 - coNP-complete 2, 5
 - context-free 279, 280
 - Δ_2^P -complete 272
 - dense 26, 265
 - disjunctively self-reducible 60
 - E-complete 275
 - EXP-complete 274, 275
 - \mathcal{F} -selective 59
 - finite 68, 219
 - FP_{total} -selective 59
 - hardness for classes *see* hardness, of sets, classifying via reductions
 - k -locally self-reducible 194
 - minimum-weight 68, 69
 - $\text{Mod}_k P$ -complete 298
 - NE-complete 275
 - near-testable 296
 - nearly near-testable 296
 - NL-complete 82, 83, 89
 - NL-complete, with respect to 1-L reductions 278
 - NP-bounded-truth-table-complete *see* set, NP-complete
 - NP-complete 1–3, 8, 9, 18–20, 22, 23, 26, 27, 31, 60, 91, 93, 95, 98, 99, 266–269, 282, 286, 287, 305
 - NP-complete ones that are non-isomorphic 284, 285
 - NP-complete, ones that are P-isomorphic 282
 - NP-complete, relativizably so 60
 - NP-conjunctive-truth-table-complete *see* set, NP-complete
 - NP-hard 1, 3, 8, 9, 18, *see* NP-hard
 - NP-hard, sparse *see* NP-hard
 - NP-many-one-complete *see* set, NP-complete
 - NP-printable 275
 - NP-Turing-complete *see* set, NP-complete
 - $NP \cap \text{coNP}$ -complete 269
 - NPSV-selective 295–297
 - of all prime numbers 131
 - of primes 277
 - P-capturable 6, 26
 - P-close 296
 - P-complete 265
 - P-printable 28, 284, 285
 - P-selective 47, 59, 64, 294–297, *see* P-sel
 - paddable 269, 282
 - padded version of 251
 - $\oplus P$ -complete 298
 - $P^{C=P}$ -complete 293
 - PL-complete 278
 - polynomial-time 264, *see* P
 - possibility of NP having sparse Turing-complete 27
 - possibility of NP having sparse Turing-hard 27
 - potential existence of sparse, in NP–P 23, 275
 - potential existence of tally, in NP–P 23, 24, 275
 - potential lack of sparse \leq_T^P -hard, for UP 284
 - $\text{Mod}_k P$ 298
 - potential lack of sparse \leq_{btt}^P -hard, for NP 9, 268
 - potential lack of sparse \leq_{btt}^P -hard, for P 265
 - potential lack of sparse \leq_{att}^P -hard, for NP 268
 - potential lack of sparse \leq_m^P -complete, for coNP 5
 - potential lack of sparse \leq_m^P -complete, for NP 8
 - potential lack of sparse \leq_m^P -hard, for coNP 5
 - potential lack of sparse \leq_T^P -complete, for NP 1, 18, 19, 268
 - potential lack of sparse \leq_T^P -hard, for NP 1, 20, 22, 60, 268
 - potential lack of tally \leq_m^P -complete, for NP 2
 - potential lack of tally \leq_m^P -hard, for NP 2

- PP-complete 293
- PSPACE-complete 87, 176, 194, 197, 272, 274
- rankable 265
- recursive 264
- self-reducible 60
- semi-feasible 45, 47–49, 51–54, 57, 59, 63, 64, *see* selectivity
- semi-feasible, nondeterministic analog of 57
- semi-recursive 295
- #L-complete 279
- #P-complete 115, 119, 286, 287
- Σ_2^P -complete 272
- small advice 47
- sparse 1–29, 269, 276, 277, 307, 308, *see* relativization, by sparse oracles, *see* SPARSE
- sparse, in NP 268, 274, 275
- sparse, in P 284, 285
- sparse, in PH 275
- supersparse 28
- tally 2, 3, 5, 6, 23, 24, 26, 274, 287, *see* TALLY
- Θ_2^P -complete 272
- Turing self-reducible 296
- UL-complete 278
- UP-hard 283, 284
- US-complete 69
- weakly P-selective 63
- ZPP-hard 288
- set-f 57–59, 61, 62, 65, 291, 292, 294, 295, 297, 306
- sets
 - disjoint 185, 246
 - P-isomorphic *see* P-isomorphism
 - sparse, lowness of *see* lowness, of sparse sets
- Sewelson, V. 22, 24, 26–29, 106, 107, 274, 275
- SF_k 176, 177, 181, 183, 185, 194, 300–303, *see* computation, bottleneck, *see* machine, bottleneck
 - closure properties *see* closure, of SF₅...
- Shamir, A. 163, 164, 270
- Sharir, M. 264
- Sherman, A. 36, 43, 44
- Sheu, M. 232
- Siefkes, D. 269
- sign function *see* function, sign
- Silvestri, R. 27, 269, 277, 285
- Simon, I. 279, 293
- Simon, J. 82, 254, 260, 273, 279, 290, 293
- simulation
 - nondeterministic, of an oracle 76
 - probabilistic, of an oracle 75
- simulation round *see* round, simulation
- single-valuedness
 - of FP 291
- Sipser, M. 163, 232, 264, 265, 269, 274, 285, 286, 288, 300
- Sivakumar, D. viii, 29, 88, 265
- Skyum, S. 302
- small circuits *see* circuits, small
- Smith, C. ix
- Solovay, R. 231, 268–270, 272, 273
- solution *see* reduction, of numbers
 - of solutions, *see* reduction, of the number of solutions
 - type *see* type, solution
 - unique 67, 68
- solvable monoid *see* monoid, solvable
- sorcerer
 - pointy-hatted vii
 - pointy-headed vii
- soundness
 - of a protocol 110, 115, 116, 118, 123, 132–138, 145, 149, 155, 299
- S₂^P 27, 64, 164, 268
- (S₂^P)^{NP} ∩ coNP 64
- space
 - exponential 264
 - logarithmic *see* C=L, *see* L, *see* NL, *see* PL, *see* UL
 - polynomial *see* PSPACE
- space hierarchy theorem *see* theorem, space hierarchy
- SpanP 104, 105, 107, 108, 297, 299
 - closure properties *see* closure, of SpanP...
- SPARSE 273, 276, 307, 308
- sparse P superset *see* superset, sparse P
- sparse set *see* set, sparse
- specification
 - unique, of a polynomial 111
 - unique, of a polynomial by coefficients 148
 - unique, of a polynomial by points 157
- Spielman, D. 89, 260
- splitting
 - of intervals 13

- SPP 100–103, 105, 106, 284, 287,
290–293, 298, *see* class, counting
– promise *see* promise, in the
definition of SPP
- Srinivasan, A. 89
- SSF_k 185, 194, 300–302, *see* machine,
symmetric bottleneck
- state
– query 110
– random starting 195
– unique accept 127
- Stearns, R. 27, 264, 275
- Stein, C. 266
- Stephan, F. 285, 296
- Stockmeyer, L. 29, 264, 270–274, 279,
281, 286, 308
- Stoness, S. ix
- storage
– safe 302
– value of 302
- straight-line program *see* program,
straight-line
- strategy
– parameterized 136
- stratified circuits *see* circuits,
stratified
- Straubing, H. viii, 193, 194, 281
- string
– Kolmogorov-easy 265
– tally 5
- strong exponential hierarchy *see*
hierarchy, strong exponential
- strongness
– of length-based honesty 37
- subcircuit 198, 203–206, 208, 211–213,
217, 223–225, 227, 228, 230, *see*
circuit
- subcircuits
– maximally disjoint 206
- subgroup 174
– commutator 167, 174, 175
- sublinear parallel access to NP *see*
access, sublinear-parallel, to NP
- subroutine
– polynomial-time 264
– unit-cost 269
- subtraction
– integer 38
– proper 91–96, 98, 99, 104–107
- succinct certificate *see* certificate,
succinct
- Sudan, M. ix, 163–166, 267, 269
- Sudborough, L. 280, 281
- Sundaram, R. 27, 164
- Sundell, S. ix
- superpolynomial-size circuits *see*
circuits, superpolynomial-size
- superset
– sparse P 26
- supersparse set *see* set, supersparse
- survey
– amusing, of the research leading to
IP=PSPACE 164
- Swier, R. viii
- switching
– quantifier 77
- Switching Lemma *see* Lemma,
Switching
- symmetric alternation *see* alternation,
symmetric, *see* S₂^p
- symmetric bottleneck machine *see*
machine, ...symmetric bottleneck...
- symmetric difference *see* difference,
symmetric
- symmetric function *see* function,
symmetric
- symmetric gate *see* gate, symmetric
- system
– bounded-round multiprover interac-
tive proof 164
– interactive proof 109–112, 114,
115, 123, 133, 164, 274, 299, 300, *see*
completeness, of a protocol, *see*
interaction, *see* IP, *see* MIP, *see* pro-
tocol, *see* prover, *see* replacement, of
provers with an oracle, *see* soundness,
of a protocol, *see* verifier
– multi-prover interactive proof *see*
MIP
– multiprover interactive proof 110,
111, 164, 299
– of elections developed in 1876 by
Lewis Carroll 272
– one-prover interactive proof 111,
299
– two-prover interactive proof 133,
135
– two-prover one-round interactive
proof 164
- Szegedy, M. 164–166, 269
- Szelepcsényi, R. 278
- Szemerédi, E. 280
- tableau method *see* method, tableau
- TALLY 307, 308
- tally set *see* set, tally
- tally string *see* string, tally

- Tamon, C. 27
- Tan, S. 279
- Tang, C. ix
- tape
 - input 250, 254, 255
 - query 110, 213, 249–251, 254–256
 - work 250, 254, 255
 - write-only 254
- Tardos, G. 29, 64
- Tarui, J. ix, 87–89, 297
- task
 - divided computation 185, 301
- Technique
 - Isolation 56, 64, 67–89, 108
 - Nonsolvable Group 167–195
 - One-Way Function 31–44
 - Polynomial 235–261
 - Polynomial Interpolation 109–166
 - Random Restriction 197–233
 - Self-Reducibility 1–29
 - Tournament Divide and Conquer 45–65
 - Witness Reduction 91–108
- technique
 - divide and conquer, in general 45, 169, 170
 - large gaps and brute force short strings 56
 - nonrelativizable proof 270
 - organization by vii
 - pruning 2
 - relativizable proof 87, 197, 259, 270
- testing
 - multilinearity 164
 - of a witness 40
- textbook
 - use of this book as viii
- Thakur, M. ix, 285
- Theorem
 - Chebyshev’s 163
 - Chinese Remainder 120
 - Cook’s 58, 59, 64, 268
 - Cook–Karp–Levin 64, *see* Theorem, Cook’s
 - Cook–Levin 64, *see* Theorem, Cook’s
 - Hartmanis–Immerman–Sewelson *see* Encoding, Hartmanis–Immerman–Sewelson
 - Karp–Lipton 20, 27, 60, 64
 - Mahaney’s 2, 26
 - Ogihara–Watanabe 26
 - PCP 165, 166
 - Prime Number 131
 - Rice’s 285
 - Savitch’s 125, 163
 - Toda’s 68, 72, 78, 87, 88, 115, 194, 259
- theorem
 - space hierarchy 22, 27
 - time hierarchy 22, 27, 264
- theorems via algorithms under hypotheses approach *see* approach, theorems via algorithms under hypotheses
- theory
 - circuit 88, *see* circuits, *see* class, circuit
 - complexity 1–308, *see* secret
 - recursive function 271, 295
 - tournament 45, 50, 51, *see* tournament
- Thérien, D. 193, 194, 260, 289
- Thierauf, T. ix, 27, 64, 108, 277, 279, 289, 297
- threshold
 - acceptance 50
 - rejection 50
- threshold circuits *see* approximation, of threshold circuits by parity circuits, *see* circuits, threshold
- threshold gate *see* gate, threshold
- time 138, 251
 - deterministic double-exponential 53
 - deterministic exponential 2, 23, *see* EXP, *see* E
 - deterministic polynomial 49, 264, *see* P
 - double exponential nondeterministic 264
 - nondeterministic exponential 2, 23, 133, *see* NEXP, *see* NE
 - nondeterministic polynomial 49, *see* NP
 - parity exponential 28
 - probabilistic polynomial 49, *see* PP
 - triple-exponential 32
 - unambiguous polynomial 283, 284, *see* UP
- time hierarchy theorem *see* theorem, time hierarchy
- Toda’s Theorem *see* Theorem, Toda’s
- Toda, S. ix, 64, 68, 78, 87–89, 108, 115, 194, 259, 279, 284, 286, 293, 296–298
- Tomer, J. ix
- Tompa, M. 82, 254, 260, 279, 280

- tongue
 - seared vii
- top gate *see* gate, top
- Torán, J. ix, 29, 88, 106, 284, 289, 293, 297–299
- Torenvliet, L. ix, 63, 287, 295, 296
- total degree *see* degree, total, of a polynomial
- total function *see* function, ...total...
- tournament 45–47, 50–52, 57, 62, *see*
 - graph, tournament
 - defeat in 45–50, 62
 - round-robin 45
- tournament graph *see* tournament
- tournament theory *see* theory, tournament
- translation
 - downward, of equality 23, 25, 28
 - upward 23, 28, 29
 - via padding 307
- traversal
 - in-order 178, 180
- tree
 - bushy 8, 56
 - computation, of a deterministic polynomial-space Turing machine 112
 - computation, of a nondeterministic Turing machine 92, 278, 281
 - disjunctive self-reducibility 5, 7
 - expanding of a 6
 - full binary 169, 177
 - full quaternary 177
 - pruning *see* procedure, self-reducibility-based tree-pruning, *see* procedure, tree-pruning
 - root of *see* root, of a tree
 - self-reducibility 5–7
- tree-pruning algorithm *see* algorithm, tree-pruning
- tree-pruning approach *see* approach, self-reducibility-based true-pruning
- Trevisan, L. ix, 166
- triple-exponential time *see* time, triple-exponential
- True 2–7, 14, 21, 178–180
- truth-table 10, 14, *see* \leq_{tt}^p , *see* condition, truth-table
- Turing self-reducible set *see* set, Turing self-reducible
- Turing, A. 264
- two-sided error *see* error, two-sided
- type
 - acceptance 108, *see* reduction, of the cardinality of acceptance types
 - finite-cardinality acceptance 108
 - solution 65
- Ukkonen, E. 26
- UL 67, 68, 82–87, 89, 278, *see* set, UL-complete
- UL/poly 68, 82–84, 278
- Ulfberg, S. 232
- Ullman, J. 264, 266
- Umans, C. ix, 272
- unambiguous function *see* function, unambiguous
- unambiguous nondeterminism *see* UL, *see* UP
- unambiguous NP machine *see* machine, unambiguous NP
- unbounded fan-in circuits *see* circuits, unbounded fan-in
- uniform distribution *see* distribution, uniform
- uniformity 281
 - logspace 281
 - NC^1 281
 - P 281
 - U_{E^*} 281
- union
 - closure of Mod_kP under *see* closure, of Mod_kP under union
 - closure of NP under *see* closure, of NP under union
 - closure of P under *see* closure, of P under union
 - closure of PP under *see* closure, of PP under union
 - disjoint 96, 185, 245
- unique accepting configuration *see* configuration, unique accepting
- universal machine *see* machine, universal
- University of Rochester *see* Rochester, University of
- UP 28, 33–36, 43, 44, 63, 67, 87, 94–102, 105–107, 263, 268, 281–285, 287, 291–293, 296, 298, *see* machine, categorical, *see* set, potential lack of spare \leq_T^p -hard, for UP, *see* set, UP-hard
 - closure properties *see* closure, of UP...
 - exponential-time analog of *see* analog, exponential-time, of UP, FewP, $\oplus P$, ZPP, RP, or BPP

- gap analog of 100
- promise *see* promise, in the definition of UP
- upward translation *see* translation, upward
- US 69, 71, 281, 283–285, 293, *see* set, US-complete

- Valiant, L. 88, 279, 282, 283, 286, 287, 302
- value
 - census 20, 49
 - maximum 104
- van der Waerden, B. 163
- van Emde Boas, P. ix, 296
- van Melkebeek, D. ix, 27, 29, 265
- Vandermonde matrix *see* matrix, Vandermonde
- variable
 - random 135, 203
- variance 135, 137, 203
- Vazirani, U. 87–89, 194
- Vazirani, V. 87, 89
- vector
 - nonzero 88
- vectors *see* reduction, of the cardinality of a set of vectors
- Venkateswaran, H. 88, 280
- Vereshchagin, N. 231, 269, 283, 285, 288
- verification
 - deterministic, of mathematical statements 109
 - mechanical, of mathematical statements 267
 - of a certificate 109
 - of accepting computation of a PSPACE machine 125
 - of an arithmetic expression 138
 - of computation of a verifier 165
 - of mathematical statements 109
 - of permanent 112
 - of primality 131, 142
 - of reachability 129
 - of satisfiability 112
 - via interactive proof systems 109
 - with $\mathcal{O}(\log n)$ random bits 166
 - with polylogarithmic random bits 165
- verifier 109, 110, 115, 123, 132–135, 163, 165, 299, 300, *see* system, interactive proof
 - polynomial-time 110
 - power of 109
- Vinay, V. 88, 279
- Vishkin, U. 279, 281, 308
- Vollmer, H. ix, 107, 194, 260, 277
- Voltaire, François Marie Arouet 268
- von Braunmühl, B. 27
- von Neumann, J. 264

- Waerden, B. van der *see* van der Waerden, B.
- Wagner, K. ix, 26, 27, 106, 107, 194, 260, 271, 272, 274, 275, 290
- wands
 - of combinatorics vii
- Wang, J. 64, 297
- Watanabe, O. ix, 26–29, 43, 63, 64, 89, 108, 276, 277, 297, 308
- weak assignments *see* assignments, weak
- weak equality *see* equality, weak
- weakly P-selective set *see* set, weakly P-selective
- Wechsung, G. ix, 26, 27, 64, 65, 106–108, 260, 274, 275, 293, 303
- weight
 - minimum 68
- WeightSum* 84–86
- West, D. 64
- Whitman, W. 274
- width
 - of PBP 167
- Wigderson, A. 28, 87, 89, 164, 166, 269, 289, 300
- Wilson, C. 28, 308
- winner
 - in an election system 272
 - of a match 45
- wisdom
 - conventional vii
- witness *see* reduction, of numbers of witnesses
 - accepting computation viewed as 94
 - length of 39, 41
 - membership 9, 10, 39–41
 - unique 282
- witness reduction *see* reduction, witness
- witness testing *see* testing, of a witness
- Wössner, H. ix
- word problem *see* problem, word
- work tape *see* tape, work
- world

- relativized 19, 27–29, 65, 107, 108, 228, 231, 232, 268–270, 282, 283, 285, 288, *see* oracle
- worst-case cryptography *see* cryptography, worst-case
- Wrathall, C. 271, 272
- Wright, E. 163
- write-only tape *see* tape, write-only

- Yao, A. 88, 232
- Yap, C. ix, 26
- Yesha, Y. 26, 28, 272, 274, 275, 285
- Young, P. 27, 269, 277, 282, 283, 296, 297

- Zachos, S. ix, 87, 269, 271, 289, 290, 297, 298, 308
- Zaki, M. 297
- Zankó, V. 163
- zero-divisor
 - of a ring 112
- zero-knowledge protocol *see* protocol, one-round perfect-zero-knowledge
- zero-polynomial 152
- Zhong, J. ix
- Zhou, S. 89
- Zimand, M. ix, 29, 43, 231, 269, 297
- Zippel, R. 163
- ZPP 22, 27, 28, 58, 61, 64, 268, 276, 277, 288–290, 294, *see* set, ZPP-hard
 - exponential-time analog of *see* analog, exponential-time, of UP, FewP, \oplus P, ZPP, RP, or BPP
- Zuckerman, D. 289