

Index

- Ajtai's paper, 183, 306
- ancestor, 66
- antecedent, 64
- atom, 11
- automatizability, 365, 459
 - essential non-, 460, 467
 - weak, 467
- axiom
 - 1-, 421
 - bounded collection, 257
 - boundedness, 191
 - comprehension, 191
 - extension, 330
 - extensionality, 187
 - non-negativity of squares, 124, 129
 - Ω_1 , 166
 - replacement, 257
 - set-boundedness, 187
- bipartite matching problem, 360
- bit length, 186
- bit-graph, 305
- Boolean
 - algebra, 453
 - axioms, 118, 128
 - circuit, 27
 - function, 12
 - monotone, 13
 - program, 85
- bounded arithmetic, 165, 191, 296
 - language of, 186
 - with exponentiation, 262
- bracket operation, 143
- branching program, 97
 - read once, 97
- broken mosquito screen, 359
- calculus
 - binomial, 350
 - Gaussian, 157
 - Hajós's, 154
 - linear, 137, 157
 - polynomial, 117, 325
 - propositional, 39
 - quantified propositional, 82
 - rationator, 1
- canonical pair, 361, 382, 459
- Cantor diagonal argument, 216
- carry-save addition, 213
- cedent, 64
- chain interpolation, 410
- characteristic function, 24
- circuit
 - algebraic, 152
 - g -, 433
 - monotone, 286, 369
 - linear programming, 407
 - real, 386
 - with local oracle, 408
 - separating, 286
- circuit class, 29
- clause, 12
 - empty, 94
 - learning, 295
- clause reduction, 424
- clause substitution, width of, 424
- clique, 29, 267
 - function, 287
- cofinal extension, 444
- communication complexity, 366
 - δ -approximate, 401
 - of set, 371
 - monotone, 371
 - real, 387
 - mono, 388
 - 3-party, 395
- complexity gap, 291
- cone, 126
- configurational refutation, 103

- conjecture
 - Cook–Reckhow, 183
 - Pudlák’s, 462
 - Razborov’s, 438, 454
 - Rudich’s, 437
- connective
 - counting, 199
 - equivalence, 14
 - implication, 14
 - modular counting, 15, 327
 - parity, 15, 17, 116
 - propositional, 11
 - threshold, 15
 - unbounded-arity, 73
- conservativity, 193, 236
- consistency formula, 417
- continuum hypothesis, 2, 189, 196
- Cook’s formula, 434
- Cook–Reckhow definition, 33, 134
- covering relation, 455
- CSP problem, 147
- cutting planes, 115, 121
 - axioms, 122
 - rules, 122
- dag, 28
- Danae gift, 327
- degree
 - Lasserre, 132
 - of graph, 277
 - of proof, 120
 - Sherali–Adams, 132
- Dehn
 - calculus, 153
 - function, 153
- DeMorgan
 - language, 11
 - laws, 15
 - rules, 94
- dependency program, 407
- depth, 307
 - logical, 17, 20
 - of formula, 58, 74
 - Σ -, 78, 296
- descriptive complexity, 471
- design, 337, 346
 - Nisan–Wigderson, 438
 - SOS, 346, 351
- deterministic acceptor, 458
- diagonalization, 463
- Diffie–Hellman scheme, 404
- discrete logarithm, 409
- disjoint NP pair, 286, 287, 353, 355
 - complete, 459
 - p-reducibility of, 459
- disjointness problem, 396
- DPLL, procedure, 95, 96
- effective interpolation, 353
- equational calculus, 116
- essential variables, 440
- Euler characteristic, 455
- expander, 277, 281
- expansion of a graph, 281
- extension
 - atom, 53
 - axiom, 53, 111
 - variable, 111
- factoring, 160
- feasibility predicate, 182
- feasible disjunction property, 383
 - strong, 383
- feasible interpolation, 72, 353, 355, 356, 476
 - construction, 355
 - history, 380
 - monotone, 355
 - property, 355
 - set-up, 354
- forcing
 - conditions, 450
 - game, 450
 - model-theoretic, 450
 - Robinson’s, 450
- forcing relation, 265
- formula
 - algebraic, 152
 - basic, 206
 - bounded, 148
 - DNF_1 -, 206, 263
 - first-order, 19
 - PHP, 35, 38
 - propositional, 11
 - quantified propositional, 81, 246
 - relativized, 84
 - satisfiable, 12
 - second-order, 21
 - strict, 192
 - τ -, 284, 426
 - unsatisfiable, 12
- Frege
 - axiom scheme, 40
 - proof, 40
 - rule, 40
 - system, 41
- Frege system, 159
 - AC^0 -, 138
 - $\text{AC}^0(\text{MOD}_m)$, 197
 - bounded depth, 58
 - BPF, 86
 - circuit, 139
 - extended, 52

512

Frege system (cont.)
 P/poly-, 138
 quantum, 160
 relativized, 84, 222
 substitution, 52
 weak PHP (WPHP), 140, 250
 with $\oplus$, 197
 with counting, 199
 function
 circuit value, 430
 iterable, 433
 truth table, 432
 Gödel's letter, 2
 Gödel's number, 460
 gadget, 430
 game, 387
 Buss–Pudlák, 44, 62, 293, 318, 335
 Ehrenfeucht–Fraïssé, 113, 289
 Karchmer–Wigderson, 366
 Prover–Delayer, 293
 Student–Teacher, 240, 258, 440
 generator
 gadget, 430, 431
 Nisan–Wigderson, 429, 438, 475
 proof complexity, 427
 exponentially hard, 427
 hard, 427
 Gomory–Chvátal cut, 122
 graph coloring, 288
 Gröbner algorithm, 406
 hard bit, 363
 hard formulas
 sequence of, 414
 set of, 414
 hardness of a function, 428
 hardness on average, 438
 Henkin construction, 170
 Herbrand function, 239
 hierarchy
 linear-time, 166, 182
 polynomial-time, 38, 183, 480
 Hilbert's
 Entscheidungsproblem, 1, 2, 32, 38
 Nullstellensatz, 119
 problems, 132
 program, 1
 ideal, 118
 ideal proof system, 151, 152
 implicit
 extended resolution, 143
 proof system, 142
 proofs, 141, 142
 independent set, 267
 inference rules, 33
 infinitesimal, 453

Index

integer hull, 130
 integer linear programming, 121, 128
 integrality conditions, 128
 interpolant, 14
 monotone, 14
 interpolating circuit, 72
 intuitionistic logic, 158
k-evaluation, 311
 Kripke semantics, 159
 language
 complete propositional, 39
 of rings, 116
 one-sorted, 189
 propositional, 116
 relational, 19, 21
 second-order, 188
 lemma
 deduction, 41, 62
 diagonal, 461, 463
 PHP switching, 314
 Schwartz–Zippel, 159
 Spira's, 17, 49, 76, 361, 368
 van Kampen's, 154
 level
 algorithmic (A-), 472
 combinatorial (C-), 473
 logical (L-), 474
 mathematical (M-), 476
 of proof complexity, 384, 472
 lift and project, 394
 lifting rules, 128
 limited extension, 93, 94
 limited recursion on notation, 233
 linear equational calculus (LEC), 137
 linear growth, 166
 linear program, 395
 linear programming, 128
 literal, 12
 Löb's conditions, 461
 logic
 compactness of, 188
 completeness of, 188
 propositional
 quantified, 159
 second-order, 20
 logical
 addition, 116
 complexity, 20
 equivalence, 14
 term, 12
 validity, 12
 Lovász–Schrijver proof system, 128
 matrix
 expander, 284
 incidence, 277

- random, 278
- sparse, 277, 284
- model
 - cut in, 170
 - non-standard, 170, 188
 - saturated, 452
 - small canonical, 445
 - standard, 170, 188
- model-completeness, 126
- modus ponens, 40
- multi-function, 255, 366, 419
 - Karchmer–Wigderson, 366
- natural proofs, 381, 433, 475, 478
- negative occurrence, 14
- normal form
 - conjunctive (CNF), 13
 - disjunctive (DNF), 13
 - negation, 16, 70, 243
- NP search problem, 87, 255, 419, 435, 469
 - GLS, 437
 - p-reducibility of, 420
 - PLS, 435
 - colored, 292, 436
 - Ramsey, 436
 - Turing reducibility, 435
- NP-complete search problem, 469
- Nullstellensatz, 115, 126
 - extended, 150, 330
 - unstructured, 150, 336
- proof system, 115, 120, 225, 325
- numeral, 148
 - dyadic, 148
- OBDD proof system, 146, 147
- one-way function, 362
 - strong, 363
- optimal proof search, 468
- p-equivalence, 34
- p-reducibility, 26
- p-simulation, 34, 181
- pairing, 186
- parameterized complexity, 471
- Paris–Harrington principle, 413, 434
- parity function, 28
- partition
 - m -, 211
 - partial, 323
- Peano arithmetic, 33, 147, 165, 262
- pebbling, 104, 289
 - black game, 289
 - black–white game, 289
 - contradiction, 289, 290
 - formula, 289
 - price, 290
 - time, 290
- perfect matching, 360
- permutation, 158
- polynomial identity testing, 159
- polynomial program, 407
- positive occurrence, 14
- Positivstellensatz, 115, 126, 132
 - proof, 127
- Pratt’s definition, 409
- prefix notation, 12
- prime factorization, 357
- principle
 - choice, 204
 - housesitting, 350
 - iteration, 350
 - least number, 195, 204
 - modular counting, 115, 211, 320, 322
 - Paris–Harrington, 413
 - pigeonhole (PHP), 35, 123, 146, 179, 277, 294, 308, 322
 - bijective, 258
 - bit PHP, 280
 - injective, 258
 - structured, 335, 436
 - surjective, 258
 - weak, 36, 215
 - Ramsey, 291, 320
 - tournament, 267, 291
 - WPHP, 250, 288, 440
 - dual, 250, 437
 - modified, 297
 - onto, 216
 - surjective, 157
- problem
 - $AC^0[p]$ -Frege, 327
 - Δ_0 -PHP, 166
 - $R(\log)$, 291, 303
 - depth d vs. $d + 1$, 291, 301, 304
 - feasible disjunction, 383
 - finite axiomatizability, 166, 479
 - finitistic consistency, 462
 - iterability, 440
 - linear generator, 429
 - NP vs. coNP, xiv, 34
 - optimality, 35, 38
 - P vs. NP, xiv, 1, 2
 - proof search, 35, 468
 - real protocols, 406
 - WPHP, 320
- proof
 - P -like, 373
 - cut-free, 65, 112
 - dag-like, 43
 - graph, 43
 - height of, 43, 66, 102, 121
 - line, 39

514

proof (cont.)
 sequence-like, 43
 step, 39
 tree-like, 42, 43, 70
 width of, 66
 proof system
 Σ -depth, 79
 completeness of, 33
 OBDD, 396
 optimal, 34
 p-bounded, 34
 p-optimal, 34
 propositional, 33
 pseudo, 161
 R-like, 206
 refutation, 94
 soundness of, 33, 174, 244
 strong, 411
 with advice, 160
 protocol, 367
 communication complexity of, 368
 consistency condition, 367
 Karchmer–Wigderson, 366, 368
 monotone, 368
 randomized, 400
 size of, 368
 tree-like, 368
 provability relation, 33
 quantifier
 bounded, 148, 169
 counting, 200
 modular counting, 197
 set bounded, 191
 sharply bounded, 192
 random formula, 413, 437
 rank
 Lovász–Schrijver, 131
 semidefinite, 131
 of a proof, 131
 of CP ref., 130
 reflection pair, 361
 reflection principle, 175–177, 361, 416
 relativization, 270
 resolution, 93, 94, 160
 DNF-, 108
 extended, 111
 height, 102
 linear, 112, 291
 narrow, 113
 over CP, 135
 over PC, 137
 pool, 295
 random, 155, 293
 refutation, 94
 regular, 97, 112

Index

rule, 93
 size, 109
 space, 102, 103, 113, 160, 294
 tree-like, 95
 width, 294
 restriction, 99
 PHP-, 314
 Riemann hypothesis, 37, 38
 Robinson’s arithmetic, 147, 186, 418, 435, 470,
 475, 477
 RSA pair, 364
 RSUV isomorphism, 196, 252
 rudimentary
 predicates, 182
 sets, 2, 166
 rule
 cut, 65
 extension, 53
 induction, 169
 quantified propositional, 82
 substitution, 52, 90
 weakening, 99
 SAT algorithm, 36, 472, 475
 SAT solving, 294
 satisfaction relation, 19, 84
 satisfiability threshold, 282
 scheme
 axiom, 33
 collection, 204
 induction, 148
 replacement, 204
 search problem, 97, 102
 semantic
 P-proof, 373
 derivation, 370, 371
 resolution, 370
 rule, 370
 semi-algebraic calculus, 124
 sequent, 64
 sequent calculus, 64, 169
 first-order, 136
 monotonic, 146
 over CP, 136
 rules, 65
 set theory, 33, 147, 188
 Shannon’s estimate, 28
 Sheffer’s stroke, 15
 similar circuits, 139
 simulation, 34
 Sipser function, 297
 size of
 Boolean program, 85
 circuit, 27
 formula, 15, 16

- Skolem
 - axiom, 248
 - function, 87, 248, 269
- Skolemization, 88, 248, 251, 269
- space complexity, 25
- span program, 391
 - monotone, 391
 - size of, 391
- sparse set, 457
- spectrum problem, 2, 457
- structure
 - Boolean-valued, 453
 - combinatorics of, 159, 455
 - expansion of, 22
 - finite, 21
 - first-order, 19
 - pseudofinite, 447
 - two-sorted, 188
 - universe of, 19
- subformula, 11
- subformula property, 68, 170
- substitution, 17, 41
 - second-order, 90, 222
- succedent, 64
- sum-of-squares, 126, 127
- Tarski's truth definition, 20
- tautology, 12
- term, 19, 116
- term unification, 59
- tertium non datur, 40
- theorem
 - Ajtai's, 318, 334
 - Atserias–Dalmau, 105, 113
 - Beth's, 72, 356
 - Buss's witnessing, 236
 - Chinese remainder, 469
 - Chvátal–Szemerédi, 282
 - Cobham's, 257
 - compactness, 442
 - completeness, 170, 269, 442
 - Cook's, 26, 475
 - Cook–Reckhow, 34
 - Craig's, 14
 - Fagin's, 21, 176
 - feasible interpolation, 107, 113, 353, 355, 357, 365, 370, 378
 - Gödel's incompleteness, 416, 418, 435, 460, 470
 - Goldreich–Levin, 363, 475
 - Hall's, 360
 - Herbrand's, 170, 236, 237, 258, 443
 - Higman's, 153
 - Immermann–Szelepcsényi, 26
 - KPT, 239, 258
 - Lyndon's, 14
 - Matiyasevich's, 414
 - Nepomnjascij's, 61, 221
 - no-gap, 303, 304
 - Parikh's, 166, 171, 445
 - PCP, 475
 - Ramsey's, 267, 291, 414, 436
 - Reckhow's, 52, 57, 62, 117
 - Savage's, 28
 - Savitch's, 26
 - space hierarchy, 26
 - time hierarchy, 25
 - Toda's, 333, 475
 - Trakhtenbrot's, 233, 447
- theory
 - Buss's, 196
 - Cook's PV, 234
 - Jeřábek's, 250
 - Parikh's, 165
 - sequential, 470
 - universal, 238
- Thue system, 350
- time complexity, 24
- translation
 - double negation, 159
 - Paris–Wilkie, 167
 - propositional, 21, 198, 200, 242
- tree
 - 3-, 323
 - decision, 31, 97, 308
 - depth of, 31
 - DNF-, 264
 - height of, 31, 308
 - inner nodes of, 31
 - k -ary, 17
 - k -, 308
 - leaves of, 31
 - path in, 31
 - PHP-, 308
 - root of, 31
- true theory, 446
- truth
 - assignment, 12
 - partial, 99
 - value, 12
- truth table function, 13
- Tseitin formula, 280, 347, 350, 396, 437
- Turing machine, 22
- unifier, 59
 - most general, 59
- unsatisfiability certificate, 380
- van Kampen diagram, 153, 160
- variable
 - extension, 328, 330

516

variable occurrence
 bounded, 19
 free, 19
width
 LEC-, 347
 linear, 400

Index

width of
 a clause, 98
 Frege proofs, 41
 resolution proofs, 98
witnessing, 87
word problem, 153