

## Index

- acceptable enumeration, 141
- accepting device, 33
- algorithm, 1
- almost everywhere, 144
- alphabet, 6
  - of constants, 24
  - of variables, 24
- analysis problem, 40
- $a$ -restriction, 245
- axiom, 24
  
- bad-luck number, 121
- binary notation, 60
- blank symbol, 79
- Blum axioms, 141
- Boolean operations, 6
- boundary marker, 79
  
- Caesar cipher, 12, 190
- capacity of place, 236
- catenation, 6
  - of languages, 7
- catenation closure, 7
  - $\lambda$ -free, 7
- characteristic function, 87
- characteristic pair, 157
- Chomsky normal form, 21, 22
- Church's thesis, 77, 78
- ciphertext, 187
  
- clause, 162
- cleartext, 187
- clique, 184
- color-family, 248
- complete grammar form, 244
- complete set, 102
  - $m$ -complete, 104
  - 1-complete, 104
- complexity, 139
  - axiomatic, 140
  - low-level, 140
- complexity class, 147
- complexity function, 141
- complexity measure, 141
  - machine-independent, 142
- composition sequence, 111
- compression theorem, 149, 150
- computational complexity, 139
- cone, 57
- conflict in Petri net, 232
- conjunctive normal form, 162
- CONSAT, 162
- context-free complete, 244
- context-free grammar, 18
- contraction, 28
- converges ( $\downarrow$ ), 87
- corresponding function, 112
- cost function, 141
- counter automaton, 73

- creative set, 105
- cryptanalysis, 189
  - initial setups for, 189
- cryptosystem, 188
  - commutative, 197
  - context-free, 196
  - context-sensitive, 196
  - knapsack, 206
  - monoalphabetic, 196
  - polyalphabetic, 196
  - public key, 196
    - RSA, 217
    - skeletal public key, 204
- cryptotext, 187
- cube-free, 38
- data encryption standard, 195
- decrypting, 187
- degree of reducibility, 102, 104, 110
- degree of set, 127
- dense pair, 248
- derivation, 13
- derivation tree, 16
- DES, 195
- deterministic language, 68
- DH-pair, 196
- diagonalization, 2
  - dilemma of, 2
- dimension of set, 127
- Diophantine, 125
  - relation, 125
  - set, 125
- diverges ( $\uparrow$ ), 87
- DOL sequence, 37
- DOL system, 36
- dovetailing, 95
- dyadic notation, 60, 98
- effective procedure, 1
- EIL system, 39
- electronic signature, 198
- emptiness problem, 54
- empty pushdown tape, 69
- empty word, 6
- enabled, 232
- encrypting, 187
- EOL system, 38
- equivalence problem, 54
- equivalent grammars, 15
- expansion, 28
- expansion spectrum, 247
- expansive nonterminal, 247
- family equivalent, 242
- final production, 32
- finite automaton, 46
  - deterministic, 46
  - equivalence of, 52
  - nondeterministic, 48
- firing in Petri net, 232
- flipping coin by telephone, 226
- gap theorem, 148
- generalized sequential machine, 54
  - deterministic, 56
- generative device, 33
- Gödel number, 84
- grammar, 14, 15
  - context-free, 18
  - context-sensitive, 18, 41
  - graph, 264
    - left-linear, 74
  - matrix, 137
  - reduced, 245
  - regular, 19
  - regular pattern, 264
  - right-linear, 74
  - selective substitution, 263
  - self-embedding, 245
- grammar form, 241, 242
- grammatical family, 242
- graph grammar, 264
- Greibach normal form, 263
- growth function, 39
- growth matrix, 40
- gsm mapping, 56
  - inverse, 56
- HALT, 103
- halting, 32, 79
- halting problem, 88
- Hilbert's tenth problem, 124
- Hill's cryptosystem, 192, 193
- IL system, 39
- inclusion problem, 54
- IND, 143
- index for set, 97
- index of function, 84
- index of Turing machine, 84
- infinity problem, 54
- interpretation, 242, 243
- intractable, 165
- key, 188
- Khachiyan's theorem, 185
- Kleene characterization, 48
- KNAPSACK, 164
- knapsack vector, 206
  - super-increasing, 206
- language, 6
  - accepted by Markov algorithm, 34
  - accepted by pushdown automaton, 68
  - accepted by systolic tree automaton, 253
  - accepted by Turing machine, 79
  - ADPDA, 68
  - AFDA, 47

- AFNA, 48
- alphabet of, 6
- commutative, 249
- context-free, 18
- counter, 73
- defined by Petri net, 238
- deterministic, 68
- D0L, 36
- DRE, 49
- EIL, 39
- EOL, 38
- exhaustive by Petri net, 238
- generated by grammar, 15
- generated by OL system, 36
- generated by Post system, 25
- IL, 39
- $k$ -testable, 75
- locally testable, 75
- OL, 36
- recursively enumerable, 18
- regular, 19
- Las Vegas algorithm, 221
- length of derivation, 13
- length of word, 6
- letter, 6
  - nonterminal, 15
  - start, 15
  - terminal, 15
- linear grammar, 244
- linear programming, 185
- literal, 162
- logarithmic space, 182
  - complete, 182
- looping, 32, 79
- $L$  systems, 35
- marking, 232
  - initial, 232
- Markov algorithm, 31, 32
- matrix grammar, 137
- Mealy machine, 56
- measure-independent, 160
- membership problem, 54, 55
- Meyer-Fischer complexity sequence, 160
- mirror image, 17
- Monte Carlo algorithm, 221
- morphism, 8
  - inverse, 57
  - letter-to-letter, 8
  - nonerasing, 8
- $m$ -reducible, 102
- $n$ -adic notation, 60
- $n$ -ary notation, 60
- neutrality, 28
- Nivat's theorem, 59
- nonspeedable, 159
- nonterminal, 15
- normalization principle of algorithms, 78
- $\mathcal{NP}$ -complete, 167
- $\mathcal{NP}$ -hard, 167
- number system, 60
  - ambiguous, 60
  - complete, 60
  - unambiguous, 60
- OL system, 36
- 1-reducible, 102
- one-time pad, 195
- oracle, 110
- padding, 103
- pairing function, 87
- parallel rewriting, 35
- partial function, 80
- partial recursive function, 80
- pebble game, 183
- pebbling, 183
- Petri net, 231
  - alive, 238
  - with multiplicities, 238
  - place-bounded, 235
  - with place capacities, 235
- place, 232
  - input, 232
  - output, 232
- plaintext, 187
- poker by telephone, 223
- polynomially bounded TM, 164, 165
- polynomially equivalent, 167
- polynomially isomorphic, 175
- polynomially reducible, 167
- polynomially space-bounded, 177
- Post (canonical) system, 24
  - pure, 25
  - reduced, 28
  - regular, 26
- Post correspondence problem, 117
  - solution of, 117
- prefix, 6
- Presburger arithmetic, 180
- primality testing, 221
- processor, 252
- production, 13, 24, 32, 36, 68
- productive set, 105
- projection of relation, 114
- protocol, 222
- public key cryptosystem, 196
  - skeletal, 204, 205
- pumping lemma, 62
  - context-free languages, 63
  - converse of, 65
  - regular languages, 62
- pumping nonterminal, 246
  - left, 246
  - right, 246
- pumping spectrum, 246
- pure Post system, 25

- pushdown automaton, 68
  - deterministic, 68, 71
- pushdown condition, 72
- quadratic nonresidue, 224
- quadratic residue, 224
- Rabin's cryptosystem, 220
- rational transduction, 75
- reachability problem, 135, 237
- reachable, 134
- reachable in Petri net, 235
- recursion theorem, 90, 91
- recursive function, 80
- recursively enumerable, 18, 93
  - complete, 102
- recursive relatedness, 147
- recursive set, 93
- reflexive transitive closure, 13
- regular-complete, 244
- regular expression, 49
  - with squaring, 176
- regular grammar, 19
- regular pattern grammar, 264
- regular Post system, 26
- regular-sufficient, 244
- repetition pair, 27
- representation in number system, 60
- rewriting rule, 13
- rewriting system, 13
- Rice's theorem, 92
- RSA cryptosystem, 217
- SA, 95
- satisfiable, 161
- selective substitution grammar, 263
- self-applicability problem, 89, 90
- semicharacteristic function, 159
- semi-Thue problem, 131
- semi-Thue system, 266
- sentential form, 123
- Shamir's algorithm, 212–216
- signature, 198
- simple set, 109
- s-m-n* theorem, 84, 85
- sparse language, 175
- speedable, 159
  - effectively, 159
- speedup theorem, 151
- state, 44, 45, 169
  - final, 46
  - initial, 46
- strong reducibility, 103
- subcreative, 159
- subset language, 240
- substitution, 53
- subword, 6
  - final, 6
  - initial, 6
- suffix, 6
- synthesis problem, 40
- systolic tree automaton, 252, 253
  - homogeneous, 255
  - stable, 257
- systolic trellis automaton, 259
  - superstable, 262
- terminal, 15
- Thue problem, 131
- Thue sequence, 37, 38
- time bound, 160, 161
  - polynomial, 161
- time-complexity, 164, 165
- total function, 80
- total recursive function, 81
- transition diagram, 47
- transition in Petri net, 232
- transition table, 46
- translation lemma, 61
- trapdoor, 199
- trapdoor pair, 213
- trellis, 259
  - homogeneous, 259
  - regular, 259
  - semihomogeneous, 259
- truth-table reducible, 110
- truth-value assignment, 161
- Turing machine, 78, 79
  - index of, 84
  - nondeterministic, 165
  - universal, 86
- Turing reducible, 110
- unary-complete, 245
- unary grammar, 244
- undecidable, 89, 139
- unicity distance, 194
- uniform effective, 86
- universal polynomial, 128
- universal Turing machine, 86
- vector addition system, 134
- Vigenère table, 11, 12
- VLSI, 251
- weak reducibility, 110
- well-formed formula, 161
- wffpc, 161
- word, 6
  - empty, 6
- word problem, 131
- yield relation, 13
  - direct, 13