Literaturverzeichnis

[AB09] S. Arora and B. Barak. *Computational Complexity*. Cambridge University Press, 2009.

[ACG+99] G. Ausiello, P. Crescenzi, G. Gambosi, V. Kann, A. Marchetti-Spaccamela, and M. Protasi. *Complexity and Approximation. Combinatorial Optimization Problems and their Approximability Properties*. Springer-Verlag, 1999.

[BC94] D.P. Bovet and P. Crescenzi. *Introduction to the Theory of Complexity*. Prentice-Hall, 1994.

[BDG88] J.L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I*. Springer-Verlag, 1988.

[BDG90] J.L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity II*. Springer-Verlag, 1990.

[Ben64] V. Beneš. Permutation groups, complexes and rearrangable multistage connecting networks. *Bell System Technical Journal*, 43:1619–1640, 1964.

[Ben65] V. Beneš. *Mathematical Theory of Connecting Networks and Telephone Traffic*. Academic Press, 1965.

[Boc58] F. Bock. An algorithm for solving "traveling-salesman" and related network optimization problems: Abstract. *Bulletin of the 14th National Meeting of the Operations Research Society of America*, page 897, 1958.

[Čer85] V. Černý. A thermodynamical approach to the traveling salesman problem: An efficient simulation algorithm. *Journal of Optimization Theory and Applications*, 45:41–55, 1985.

[Cha66] G.J. Chaitin. On the length of programs for computing finite binary sequences. *Journal of the ACM*, 13:407–412, 1966.

[Cha69] G.J. Chaitin. On the simplicity and speed of programs for computing definite sets of natural numbers. *Journal of the ACM*, 16:407–412, 1969.

[Cha74] G.J. Chaitin. Information-theoretic limitations of formal systems. *Journal of the ACM*, 13:403–424, 1974.

[Chu36] A. Church. An undecidable problem in elementary number theory. *American Journal of Mathematics*, 58:345–363, 1936.

[CLR90] T. Cormen, C. Leiserson, and R.L. Rivest. *Introduction to Algorithms*. MIT Press and McGraw-Hill, 1990.

J. Hromkovič, *Theoretische Informatik,*
DOI 10.1007/978-3-658-06433-4, © Springer Fachmedien Wiesbaden 2014

[Coo71] S. Cook. The complexity of theorem-proving procedures. In *Proceedings of 3rd ACM Symposium on Theory of Computing*, pages 151–157, 1971.

[Cro58] G.A. Croes. A method for solving traveling-salesman problems. *Operations Research*, 6:791–812, 1958.

[DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[DK02] H. Delfs and H. Knebl. *Introduction to Cryptography.* Springer-Verlag, 2002.

[EP00] K. Erk and L. Priese. *Theoretische Informatik (Eine umfassende Einführung).* Springer-Verlag, 2000.

[GJ79] M. Garey and D. Johnson. *Computers and Intractability.* Freeman, 1979.

[GKP94] R. Graham, D. Knuth, and O. Patashnik. *Concrete Mathematics.* Addison-Wesley, 2nd edition, 1994.

[GMR85] S. Goldwasser, S. Micali, and C. Rackoff. Knowledge complexity of interactive proofs. In *Proceedings of the 17th ACM Symposium on Theory of Computation*, pages 291–304. ACM, 1985.

[Göd31] K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme. *Monatshefte für Mathematik und Physik*, 38:173–198, 1931.

[Gra66] R. Graham. Bounds for certain multiprocessor anomalies. *Bell System Technical Journal*, 45:1563–1581, 1966.

[Har93] D. Harel. *Algorithmics. The Spirit of Computing.* Addison-Wesley, 1993.

[HKMP96] J. Hromkovič, R. Klasing, B. Monien, and R. Peine. Dissemination of information in interconnection networks. In *Combinational Network Theory*, pages 125–212, 1996.

[HKP+05] J. Hromkovič, R. Klasing, A. Pelc, P. Ružička, and W. Unger. *Dissemination of Information in Communication Networks. Broadcasting, Gossiping, Leader Election and Fault-Tolerance.* Springer-Verlag, 2005.

[HMU06] J.E. Hopcroft, R. Motwani, and J.D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley, 3rd edition, 2006.

[Hoc97] D.S. Hochbaum. *Approximation Algorithms for NP-hard Problems.* PWS Publishing Company, 1997.

[Hro97] J. Hromkovič. *Communication Complexity and Parallel Computing.* Springer-Verlag, 1997.

[Hro04a] J. Hromkovič. *Algorithmics for Hard Problems. Introduction to Combinatorial Optimization, Randomization, Approximation and Heuristics*. Springer-Verlag, 2nd edition, 2004.

[Hro04b] J. Hromkovič. *Randomisierte Algorithmen. Methoden zum Entwurf von zufallsgesteuerten Systemen für Einsteiger*. B.G. Teubner, 2004.

[HS65] J. Hartmanis and R.E. Stearns. On the computational complexity of algorithms. *Transactions of AMS*, 117:285–306, 1965.

[HSL65] J. Hartmanis, R. Stearns, and P. Lewis. Hierarchies of memory limited computations. In *Proceedings of 6th IEEE Symposium on Switching Circuit Theory and Logical Design*, pages 179–190, 1965.

[HU79] J.E. Hopcroft and J.D. Ullman. *Introduction to Automata Theory, Languages, and Computation*. Addison-Wesley, 1979.

[IK74] O.H. Ibarra and C.E. Kim. Fast approximation algorithms for the knapsack and sum of subsets problem. *Journal of the ACM*, 21:294–303, 1974.

[Kar72] R.M. Karp. Reducibility among combinatorial problems. In R. Miller, editor, *Complexity of Computer Computation*, pages 85–104. Plenum Press, 1972.

[Kar91] R.M. Karp. An introduction to randomized algorithms. *Discrete Applied Mathematics*, 34:165–201, 1991.

[KGV83] S. Kirkpatrick, P.D. Gellat, and M.P. Vecchi. Optimization by simulated annealing. *Science*, 220:671–680, 1983.

[Kle36] S.C. Kleene. General recursive functions of natural numbers. *Mathematische Annalen*, 112:727–742, 1936.

[Kol65] A.N. Kolmogorov. Three approaches for defining the concept of information quantity. *Probl. Information Transmission*, 1:1–7, 1965.

[Kol68] A.N. Kolmogorov. Logical basis for information theory and probability theory. *IEEE Transactions on Information Theory*, 14:662–664, 1968.

[Lei92] F.T. Leighton. *Introduction to Parallel Algorithms and Architectures: Arrays, Trees, Hypercubes*. Morgan Kaufmann Publ. Inc., 1992.

[Lev73] L.A. Levin. Universal sorting problems. *Problems of Information Transmission*, 9:265–266, 1973.

[LP78] H.R. Lewis and Ch.H. Papadimitriou. The efficiency of algorithms. *Scientific American*, 238(1), 1978.

[LV93] M. Li and P.M.B. Vitányi. *An Introduction to Kolmogorov Complexity and Its Applications*. Springer-Verlag, 1993.

[MPS98] E.W. Mayr, H.J. Prömel, and A. Steger, editors. *Lectures on Proof Verification and Approximation Algorithms*. Number 1967 in Lecture Notes in Computer Science. Springer-Verlag, 1998.

[MR95] R. Motwani and P. Raghavan. *Randomized Algorithms*. Cambridge University Press, 1995.

[MRR+53] N. Metropolis, A.W. Rosenbluth, M.N. Rosenbluth, A.H. Teller, and E. Teller. Equation of state calculation by fast computing machines. *Journal of Chemical Physics*, 21:1087–1091, 1953.

[Pap94] Ch.H. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994.

[Pos36] E. Post. Finite combinatory process-formulation. *Journal of Symbolic Logic*, 1:103–105, 1936.

[Pos46] E. Post. A variant of a recursively unsolvable problem. *Transactions of AMS*, 52:264–268, 1946.

[PS82] Ch.H. Papadimitriou and K. Steiglitz. *Combinatorial Optimization: Algorithms and Complexity*. Prentice-Hall, 1982.

[Rei90] R. Reischuk. *Einführung in die Komplexitätstheorie*. B.G. Teubner, 1990.

[Ric53] H.G. Rice. Classes of recursively enumerable sets and their decision problems. *Transactions of AMS*, 89:25–59, 1953.

[Rog67] H. Rogers. *Theory of Recursive Functions and Effective Computability*. McGraw-Hill, 1967.

[RSA78] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–12, 1978.

[Sal73] A. Salomaa. *Formal Languages*. Academic Press, 1973.

[Sal96] A. Salomaa. *Public-Key Cryptography*. Springer-Verlag, 1996.

[SC79] L.J. Stockmeyer and A.K. Chandra. Intrinsically difficult problems. *Scientific American*, 240(5), 1979.

[Sch95] U. Schöning. *Perlen der Theoretischen Informatik*. BI-Wissenschaftsverlag, 1995.

[Sch01] U. Schöning. *Algorithmik*. Spektrum Akademischer Verlag, 2001.

[Sha92] A. Shamir. IP = PSPACE. *Journal of the ACM*, 39:869–877, 1992.

[Sip97] M. Sipser. *Introduction to the Theory of Computation*. PWS Publishing Company, 1997.

[Tra63] B.A. Trakhtenbrot. *Algorithms and Automatic Computing Machines*. D.C. Heath & Co., 1963.

[Tur36] A.M. Turing. On computable numbers with an application to the Entscheidungsproblem. In *Proceedings of the London Mathematical Society*, volume 42 of *2*, pages 230–265, 1936.

[Vaz01] V. Vazirani. *Approximation Algorithms*. Springer-Verlag, 2001.

[Wak68] A. Waksman. A permutation network. *Journal of the ACM*, 15:159–163, 1968.

[Weg05] I. Wegener. *Theoretische Informatik – eine algorithmenorientierte Einführung*. B.G. Teubner, 2005.

Index

ableitbar 292
Ableitung 292
Ableitungsbaum 312
Ableitungsregeln 291
Ableitungsschritt 292
Abzählbarkeit 128
Adjazenzmatrix 16, 187, 219
Adleman 268, 286, 342
Äquivalenzproblem 26, 255
algorithmisch erkennbar 98
Algorithmus 24, 91
    Approximations- 225
    AQP 256
    Aufzählungs- 32
    DPR 222
    Greedy- 240
    LS(f) 232
    LS-CUT 233
    Metropolis- 237
    pseudopolynomieller 219
    randomisierter 246
    SA(f) 238
    SB 228
    Solovay-Strassen- 253
    VCA 225
    zulässiger 225
Alphabet 14
Approximationsalgorithmus 225
Approximationsgüte 225
ASCII 35
Authentizitätsproblem 271

Beneš-Netzwerk 281
Berechnungsbaum 77, 116
Beweiser 273
Beweissystem 285
    interaktives 273f, 276
    Zero-Knowledge- 276, 285
Beweisverifikation 191
Bin(·) 15
Bisektion 285
Bisektionsbreite 285
Blanksymbol 95
Boole'sche Formel 14, 197, 289
Buchstabe 14

CAESAR 265
Chomsky 12, 335
Chomsky-Normalform 315
Church 112, 121, 339
Church'sche These 112, 128, 332
Clique 30, 206
Compilerbau 287, 335
COMPOSITE 193
Cook 199, 213, 340

Demokrit 241
Determinismus 242
Diagonalisierungsmethode 132
Diagonalsprache 133
Diffie 286
digitale Unterschrift 264, 270
Divide and Conquer 188
DLOG 174
Dreiecksungleichung 29
3SAT 206, 209
dynamische Programmierung 220

EA 51, 75
Echtzeit 328
Einstein 241
Einweg-Funktion 265f, 268, 285
endlicher Automat 51, 75
    Darstellung 49

J. Hromkovič, *Theoretische Informatik,*
DOI 10.1007/978-3-658-06433-4, © Springer Fachmedien Wiesbaden 2014

nichtdeterministischer 76
entscheidbar 97
Entscheidungsproblem 24
semantisch nichttriviales 145
Entschlüsselung 264
Epikur 241
Ereignis 242
atomares 242
elementares 242
ERF 26
Erweiterung 209
erzeugte Sprache 292
Euler'sche Funktion 268
EXPTIME 174

Faktorisierung 268, 285
Fehlerwahrscheinlichkeit 245, 248, 254ff
Fermat 243, 251
Fingerabdruck 254, 256

Gleichverteilung 244
Gödel 163
Goldwasser 286
Grammatik 287, 291, 332, 335
kontextfreie 297, 310
kontextsensitive 297
normierte 304
normierte kontextfreie 317
reguläre 297, 299
Typ-0- 297
Typ-1- 297
Typ-2- 297
Typ-3- 297
Graphenisomorphie 274
Greedy-Algorithmus 240
Greibach-Normalform 315

Halteproblem 140
Hamiltonscher Kreis 25, 28, 193, 224
Hellman 286
Hilbert 128, 163
Hilbert'sches Hotel 128, 131
HK 25, 224
Homomorphismus 23, 119, 151, 299

ILP 31
Implementierung der Rekursion 335
In(·) 178
Informatik 1
InKonf(·) 178, 184f
innere Konfiguration 178
IP 274
isomorph 274
Isomorphismus 274

kanonische Ordnung 19, 128
Kardinalität 19
Keller 288, 322
Kellerautomat 322, 335
nichtdeterministischer 323
Kett(·) 304
Kettenregel 304
Klartext 264
Klausel 31, 206
Kleene 20, 121
Kleene'scher Stern 20, 299
KNF 31
Knotenüberdeckung 30, 206
Kod_L 148
KodTM 119
Kolmogorov 34, 243
Kolmogorov-Komplexität 34, 73, 157
einer natürlichen Zahl 37
Kommunikation 263, 277
Kommunikationsprotokoll 271
Kommunikationsweg 278
Komplement 20, 136, 299
Komplexitätsklassen 174
Komplexitätsmaße 168
nichtdeterministische 182
Komprimierung 33
Konfiguration
einer MTM 105
einer NTM 113
einer TM 96
eines EA 53
eines NEA 76
eines NPdA 324
innere 178
Konkatenation 18, 299

kontextfrei 297
kontextsensitiv 297, 335
Kostenmaß
    logarithmisches 174, 253
    uniformes 174
Kryptoanalyse 264
Kryptographie 263f, 286
Kryptologie 264
Kryptosystem 264
    klassisches 264f
    Public-Key- 266, 271
    symmetrisches 265
Kryptotext 264

$L_{2\text{diag}}$ 134
L_{3a} 294
Last-in-first-out 322
$\mathcal{L}_{\text{CF}}$ 310
L_{diag} 133, 205
$(L_{\text{diag}})^{\complement}$ 137
$\mathcal{L}_{\text{EA}}$ 53, 99, 299
leere Sprache 20
leeres Wort 14
Lemma von Ogden 320
L_{empty} 142, 145
$(L_{\text{empty}})^{\complement}$ 142f
L_{EQ} 144
L_{ge} 293, 311, 316
L_{gleich} 106, 172
L_{H} 140
$(L_{\text{H}})^{\complement}$ 144
$L_{\text{H},\lambda}$ 145
Linksableitung 313
$L_{k,\text{diag}}$ 134
L_{Mitte} 99, 172
$\mathcal{L}_{\text{NEA}}$ 80
Logarithmus
    diskreter 267, 285
lokale Suche 232
lokales Optimum 231
L_{Pal} 311
$L_{\mathcal{P}}$ 102, 172
L_{quad} 116
L_R 326
$\mathcal{L}_{\text{R}}$ 98
$\mathcal{L}_{\text{RE}}$ 97, 125, 333
L_{Rev} 311
L_{U} 138
$(L_{\text{U}})^{\complement}$ 144
L_{ungleich} 114

Maschinencode 34, 111
Matching 225
MAX-CL 30
MAX-CUT 211, 233
MAX-SAT 31
MaxInt 219, 235
Methode
    der Diagonalisierung 132
    der dynamischen Programmierung 220
    der Fingerabdrücke 254, 259
    der häufigen Zeugen 250, 259
    der Kolmogorov-Komplexität 157
    der Reduktion 134
Metropolis-Algorithmus 237
Micali 286
MIN-VC 30, 226
Modularität 278, 285
MPKP 151
MTM 104, 174

Nachbarschaft 231
    echte 236
    polynomiell untersuchbare 235
NEA 76
Netz 277
Netzwerk 279
    Beneš- 281
Netzwerkdesign 285
Nichtdeterminismus 75, 113
NICHTISO 274
Nichtterminalalphabet 291
Nichtterminale 290
Nichtterminalsymbole 290
NLOG 183
Normalform
    Chomsky- 315
    Greibach- 315

konjunktive 31
NP 183, 190, 194, 273
NP-schwer 195, 212, 223, 236
stark 223, 236
NP-Schwere 211f
starke 239
NP-vollständig 195
NP-Vollständigkeit 205
NPdA 323
NPO 210
NPSPACE 183
NTM 113
Nummer(·) 15
nutzloses Symbol 314

O-Notation 171
Ogden 320
Optimierungsproblem 28
kostenbeschränktes 235

P 174, 181, 190, 194
Palindrom 311
Permutation 278f
Permutationsnetzwerk 279, 281
PKP 149
platzkonstruierbar 176
PO 211
Polynome 255
polynomialzeit-reduzierbar 182
Post 121, 149, 342
Post'sches Korrespondenzproblem 149
modifiziertes 151
Potenzmenge 19
Potenzmengenkonstruktion 80
Präfix 19
Prim(·) 40, 246
Primzahlsatz 41, 246
Primzahltest 25, 250, 253, 259
Produktionen 291
Programmverifikation 160
Protokoll
kryptographisches 3, 264
zufallsgesteuertes 246
PSPACE 174
Pumping-Lemma
für kontextfreie Sprachen 316
für reguläre Sprachen 70
Pumpingtechnik 70, 335

Quantenrechner 7, 112

Rackoff 286
REACHABLE 189
Rechtsableitung 313
Reduktion 134
EE- 135
polynomielle 195
rekursive 134
Regeln 291
regulär 53, 297, 308
rekursiv 25, 97, 126
rekursiv aufzählbar 97
Relationsproblem 26
Rényi 241
Reversal 18
Riemann'sche Hypothese 41
Rivest 268, 286, 339, 342
RSA 268f, 271
Rucksack-Problem 220

SAT 205
Satz
des Pythagoras 92
Primzahl- 41, 246
von Cantor und Bernstein 126
von Cook 199
von Euler 268
von Fermat 251
von Rice 146
von Savitch 188
von Shamir 275
Satzform 291
Schaltungsknoten 278
Schlüssel 264
Schmetterling 280
r-dimensionaler 281
Schwellenwert-Sprache 212
Shamir 268, 275, 286, 342
Simulated Annealing 236
Simulation 63

Spannbaum 30, 228
Speicherplatzkomplexität 168
Sprache 20
    entscheidbare 97
    kontextfreie 311
    leere 20
    reguläre 53, 308
    rekursive 97
    universelle 138
Startnichtterminal 291
Startsymbol 291
Stirling'sche Formel 280
Suffix 19
Syntaxbaum 312

Teile und Herrsche 188
Teilwort 19
Telefonnetze 286
Terminalalphabet 291
Terminalsymbole 290
TM 94, 332
Top-Symbol 322
total berechenbar 98
TSP 28, 224, 227
    metrisches 29, 229
Turing 93, 122, 164, 343
Turingmaschine 94, 332
    Mehrband- 104, 174
    nichtdeterministische 113
    universelle 138

Umkehrung 18

Verifizierer 192, 273
Verkettung 18
Verschlüsselung 264
von-Neumann-Maschine 168
VP 192, 274

Wahrscheinlichkeit 243
Wahrscheinlichkeitsraum 244
Wahrscheinlichkeitstheorie 242
Wahrscheinlichkeitsverteilung 244
Wort 14
    Länge 14
    leeres 14

Zahlproblem 219
Zeitkomplexität 168
zeitkonstruierbar 176
Zertifikat 191
Zeuge 191, 249, 256, 259
zufällig 39
Zufall 13, 39, 241
Zufallssteuerung 242