

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
1.1	Informatik als wissenschaftliche Disziplin . . . . .	1
1.2	Eine faszinierende Theorie . . . . .	5
1.3	Für die Studierenden . . . . .	8
1.4	Aufbau des Lehrmaterials . . . . .	10
<b>2</b>	<b>Alphabete, Wörter, Sprachen und die Darstellung von Problemen</b>	<b>13</b>
2.1	Zielsetzung . . . . .	13
2.2	Alphabete, Wörter und Sprachen . . . . .	14
2.3	Algorithmische Probleme . . . . .	24
2.4	Kolmogorov-Komplexität . . . . .	33
2.5	Zusammenfassung und Ausblick . . . . .	45
<b>3</b>	<b>Endliche Automaten</b>	<b>49</b>
3.1	Zielsetzung . . . . .	49
3.2	Die Darstellungen der endlichen Automaten . . . . .	49
3.3	Simulationen . . . . .	63
3.4	Beweise der Nichtexistenz . . . . .	68
3.5	Nichtdeterminismus . . . . .	75
3.6	Zusammenfassung . . . . .	86
<b>4</b>	<b>Turingmaschinen</b>	<b>91</b>
4.1	Zielsetzung . . . . .	91
4.2	Auszug aus der Geschichte . . . . .	92
4.3	Das Modell der Turingmaschine . . . . .	94
4.4	Mehrband-Turingmaschinen und Church'sche These . . . . .	103
4.5	Nichtdeterministische Turingmaschinen . . . . .	113
4.6	Kodierung von Turingmaschinen . . . . .	118
4.7	Zusammenfassung . . . . .	120
<b>5</b>	<b>Berechenbarkeit</b>	<b>125</b>
5.1	Zielsetzung . . . . .	125
5.2	Die Methode der Diagonalisierung . . . . .	126
5.3	Die Methode der Reduktion . . . . .	134
5.4	Der Satz von Rice . . . . .	145
5.5	Das Post'sche Korrespondenzproblem . . . . .	149
5.6	Die Methode der Kolmogorov-Komplexität . . . . .	157
5.7	Folgen für die Forschung . . . . .	160
5.8	Zusammenfassung . . . . .	163

<b>6</b>	<b>Komplexitätstheorie</b>	<b>167</b>
6.1	Zielsetzung . . . . .	167
6.2	Komplexitätsmaße . . . . .	168
6.3	Komplexitätsklassen und die Klasse P . . . . .	174
6.4	Nichtdeterministische Komplexitätsmaße . . . . .	182
6.5	Die Klasse NP und Beweisverifikation . . . . .	190
6.6	NP-Vollständigkeit . . . . .	194
6.7	Zusammenfassung . . . . .	213
<b>7</b>	<b>Algorithmik für schwere Probleme</b>	<b>217</b>
7.1	Zielsetzung . . . . .	217
7.2	Pseudopolynomielle Algorithmen . . . . .	219
7.3	Approximationsalgorithmen . . . . .	225
7.4	Lokale Suche . . . . .	231
7.5	Simulated Annealing . . . . .	236
7.6	Zusammenfassung . . . . .	239
<b>8</b>	<b>Randomisierung</b>	<b>241</b>
8.1	Zielsetzung . . . . .	241
8.2	Elementare Wahrscheinlichkeitstheorie . . . . .	242
8.3	Ein randomisiertes Kommunikationsprotokoll . . . . .	246
8.4	Die Methode der häufigen Zeugen und der randomisierte Primzahltest . . . . .	249
8.5	Die Methode der Fingerabdrücke und die Äquivalenz von zwei Polynomen . . . . .	254
8.6	Zusammenfassung . . . . .	259
<b>9</b>	<b>Kommunikation und Kryptographie</b>	<b>263</b>
9.1	Zielsetzung . . . . .	263
9.2	Klassische Kryptosysteme . . . . .	264
9.3	Public-Key-Kryptosysteme und RSA . . . . .	265
9.4	Digitale Unterschriften . . . . .	270
9.5	Interaktive Beweissysteme und Zero-Knowledge-Beweise . . . . .	273
9.6	Entwurf eines Kommunikationsnetzes . . . . .	277
9.7	Zusammenfassung . . . . .	285
<b>10</b>	<b>Grammatiken und Chomsky-Hierarchie</b>	<b>287</b>
10.1	Zielsetzung . . . . .	287
10.2	Das Konzept der Grammatiken . . . . .	289
10.3	Reguläre Grammatiken und endliche Automaten . . . . .	299
10.4	Kontextfreie Grammatiken und Kellerautomaten . . . . .	310
10.5	Allgemeine Grammatiken und Turingmaschinen . . . . .	332
10.6	Zusammenfassung . . . . .	335

Theoretische Informatik

Formale Sprachen, Berechenbarkeit,

Komplexitätstheorie, Algorithmik, Kommunikation und

Kryptographie

Hromkovič, J.

2014, XVIII, 349 S. 87 Abb., Softcover

ISBN: 978-3-658-06432-7