

Inhalt

1	Einleitung	15
1.1	Informatik als wissenschaftliche Disziplin	15
1.2	Eine faszinierende Theorie	20
1.3	Für die Studierenden	24
1.4	Aufbau des Lehrmaterials	27
2	Alphabete, Wörter, Sprachen und Aufgaben	30
2.1	Zielsetzung	30
2.2	Alphabete, Wörter und Sprachen	31
2.3	Algorithmische Probleme	43
2.4	Kolmogorov-Komplexität	54
2.5	Zusammenfassung und Ausblick	69
3	Endliche Automaten	71
3.1	Zielsetzung	71
3.2	Die Darstellungen der endlichen Automaten	72
3.3	Simulationen	83
3.4	Beweise der Nichtexistenz	86
3.5	Nichtdeterminismus	95
3.6	Zusammenfassung	108
4	Turingmaschinen	111
4.1	Zielsetzung	111
4.2	Das Modell der Turingmaschine	112

	Inhalt
12	
4.3	Mehrband-Turingmaschinen und Church'sche These 123
4.4	Nichtdeterministische Turingmaschinen 134
4.5	Kodierung von Turingmaschinen 140
4.6	Zusammenfassung 143
5	Berechenbarkeit 146
5.1	Zielsetzung 146
5.2	Die Methode der Diagonalisierung 147
5.3	Die Methode der Reduktion 157
5.4	Satz von Rice 170
5.5	Das Post'sche Korrespondenzproblem 174
5.6	Die Methode der Kolmogorov-Komplexität 184
5.7	Zusammenfassung 188
6	Komplexitätstheorie 190
6.1	Zielsetzung 190
6.2	Komplexitätsmaße 192
6.3	Komplexitätsklassen und die Klasse P 199
6.4	Nichtdeterministische Komplexitätsmaße 208
6.5	Die Klasse NP und Beweisverifikation 216
6.6	NP-Vollständigkeit 221
6.7	Zusammenfassung 243
7	Algorithmik für schwere Probleme 245
7.1	Zielsetzung 245
7.2	Pseudopolynomielle Algorithmen 247
7.3	Approximationsalgorithmen 254
7.4	Lokale Suche 262
7.5	Simulated Annealing 268
7.6	Zusammenfassung 272

Inhalt		13
8	Randomisierung	274
8.1	Zielsetzung	274
8.2	Elementare Wahrscheinlichkeitstheorie	276
8.3	Ein randomisiertes Kommunikationsprotokoll	280
8.4	Die Methode der häufigen Zeugen und der randomisierte Primzahltest	284
8.5	Die Methode der Fingerabdrücke und die Äquivalenz von zwei Polynomen	290
8.6	Zusammenfassung	297
9	Kommunikation und Kryptographie	299
9.1	Zielsetzung	299
9.2	Klassische Kryptosysteme	300
9.3	Public-Key-Kryptosysteme und RSA	302
9.4	Digitale Unterschriften	308
9.5	Interaktive Beweissysteme und Zero-Knowledge-Beweise . . .	312
9.6	Entwurf eines Kommunikationsnetzes	317
9.7	Zusammenfassung	327
	Literaturverzeichnis	329
	Sachverzeichnis	333