

Juraj Hromkovič

# Theoretische Informatik

**Formale Sprachen,  
Berechenbarkeit,  
Komplexitätstheorie, Algorithmik,  
Kommunikation und  
Kryptographie**

3., überarbeitete und erweiterte Auflage



Teubner

# Inhalt

<b>1</b>	<b>Einleitung</b>	<b>17</b>
1.1	Informatik als wissenschaftliche Disziplin . . . . .	17
1.2	Eine faszinierende Theorie . . . . .	22
1.3	Für die Studierenden . . . . .	26
1.4	Aufbau des Lehrmaterials . . . . .	29
<b>2</b>	<b>Alphabete, Wörter, Sprachen und Aufgaben</b>	<b>32</b>
2.1	Zielsetzung . . . . .	32
2.2	Alphabete, Wörter und Sprachen . . . . .	33
2.3	Algorithmische Probleme . . . . .	45
2.4	Kolmogorov-Komplexität . . . . .	56
2.5	Zusammenfassung und Ausblick . . . . .	71
<b>3</b>	<b>Endliche Automaten</b>	<b>75</b>
3.1	Zielsetzung . . . . .	75
3.2	Die Darstellungen der endlichen Automaten . . . . .	76
3.3	Simulationen . . . . .	93
3.4	Beweise der Nichtexistenz . . . . .	99
3.5	Nichtdeterminismus . . . . .	108
3.6	Zusammenfassung . . . . .	121
<b>4</b>	<b>Turingmaschinen</b>	<b>125</b>
4.1	Zielsetzung . . . . .	125
4.2	Das Modell der Turingmaschine . . . . .	126

4.3	Mehrband-Turingmaschinen und Church'sche These . . . . .	137
4.4	Nichtdeterministische Turingmaschinen . . . . .	148
4.5	Kodierung von Turingmaschinen . . . . .	154
4.6	Zusammenfassung . . . . .	157
<b>5</b>	<b>Berechenbarkeit</b>	<b>161</b>
5.1	Zielsetzung . . . . .	161
5.2	Die Methode der Diagonalisierung . . . . .	162
5.3	Die Methode der Reduktion . . . . .	172
5.4	Satz von Rice . . . . .	185
5.5	Das Post'sche Korrespondenzproblem . . . . .	190
5.6	Die Methode der Kolmogorov-Komplexität . . . . .	199
5.7	Zusammenfassung . . . . .	203
<b>6</b>	<b>Komplexitätstheorie</b>	<b>206</b>
6.1	Zielsetzung . . . . .	206
6.2	Komplexitätsmaße . . . . .	208
6.3	Komplexitätsklassen und die Klasse P . . . . .	215
6.4	Nichtdeterministische Komplexitätsmaße . . . . .	224
6.5	Die Klasse NP und Beweisverifikation . . . . .	231
6.6	NP-Vollständigkeit . . . . .	236
6.7	Zusammenfassung . . . . .	259
<b>7</b>	<b>Algorithmik für schwere Probleme</b>	<b>262</b>
7.1	Zielsetzung . . . . .	262
7.2	Pseudopolynomielle Algorithmen . . . . .	264
7.3	Approximationsalgorithmen . . . . .	271
7.4	Lokale Suche . . . . .	279
7.5	Simulated Annealing . . . . .	285
7.6	Zusammenfassung . . . . .	289

Inhalt		15
<b>8</b>	<b>Randomisierung</b>	<b>292</b>
8.1	Zielsetzung . . . . .	292
8.2	Elementare Wahrscheinlichkeitstheorie . . . . .	294
8.3	Ein randomisiertes Kommunikationsprotokoll . . . . .	298
8.4	Die Methode der häufigen Zeugen und der randomisierte Primzahltest . . . . .	302
8.5	Die Methode der Fingerabdrücke und die Äquivalenz von zwei Polynomen . . . . .	308
8.6	Zusammenfassung . . . . .	315
<b>9</b>	<b>Kommunikation und Kryptographie</b>	<b>318</b>
9.1	Zielsetzung . . . . .	318
9.2	Klassische Kryptosysteme . . . . .	319
9.3	Public-Key-Kryptosysteme und RSA . . . . .	321
9.4	Digitale Unterschriften . . . . .	327
9.5	Interaktive Beweissysteme und Zero-Knowledge-Beweise . . .	331
9.6	Entwurf eines Kommunikationsnetzes . . . . .	336
9.7	Zusammenfassung . . . . .	346
<b>10</b>	<b>Grammatiken und Chomsky-Hierarchie</b>	<b>348</b>
10.1	Zielsetzung . . . . .	348
10.2	Das Konzept der Grammatiken . . . . .	350
10.3	Reguläre Grammatiken und endliche Automaten . . . . .	362
10.4	Kontextfreie Grammatiken und Kellerautomaten . . . . .	376
10.5	Allgemeine Grammatiken und Turingmaschinen . . . . .	402
10.6	Zusammenfassung . . . . .	405
	<b>Literaturverzeichnis</b>	<b>408</b>
	<b>Sachverzeichnis</b>	<b>413</b>