

Inhaltsverzeichnis

| | | |
|----------|---|-----------|
| 1 | Algorithmen und Komplexität | 1 |
| 2 | Sortieren | 5 |
| 2.1 | Insertionsort | 6 |
| 2.2 | Quicksort | 9 |
| 2.3 | Heapsort | 14 |
| 2.4 | Mergesort | 24 |
| 2.5 | Mergesort iterativ | 30 |
| 2.6 | Natural Mergesort | 33 |
| 2.7 | Shellsort | 36 |
| 2.8 | Untere Schranken für das Sortieren | 43 |
| 2.9 | Bucket Sort und Radix Sort | 44 |
| 2.10 | Median-Algorithmus | 45 |
| 2.11 | Aufgaben | 52 |
| 3 | Textsuche | 55 |
| 3.1 | Textsuchproblem | 55 |
| 3.2 | Naiver Algorithmus | 59 |
| 3.3 | Nicht ganz so naiver Algorithmus | 62 |
| 3.4 | Knuth-Morris-Pratt-Algorithmus | 65 |
| 3.5 | Boyer-Moore-Algorithmus | 71 |
| 3.6 | Modifizierter Boyer-Moore-Algorithmus | 79 |
| 3.7 | Horspool-Algorithmus | 81 |
| 3.8 | Sunday-Algorithmus | 83 |
| 3.9 | Skip-Search-Algorithmus | 85 |

| | | |
|----------|--|------------|
| 3.10 | Shift-And-Algorithmus | 89 |
| 3.11 | Aufgaben | 92 |
| 4 | Graphenalgorithmen | 95 |
| 4.1 | Breitensuche | 96 |
| 4.2 | Graph als Datenstruktur | 102 |
| 4.3 | Zusammenhangskomponenten eines Graphen | 111 |
| 4.4 | Zweifacher Zusammenhang | 117 |
| 4.5 | Floyd-Warshall-Algorithmus | 124 |
| 4.6 | Minimaler Spannbaum..... | 126 |
| 4.7 | Kürzeste Wege | 133 |
| 4.8 | Dijkstra-Algorithmus | 138 |
| 4.9 | Travelling-Salesman-Problem | 139 |
| 4.10 | Faktor-2-Annäherungsverfahren..... | 140 |
| 4.11 | Simulated Annealing | 143 |
| 4.12 | Selbstorganisierende Karte..... | 146 |
| 4.13 | Aufgaben | 148 |
| 5 | Algorithmische Geometrie | 151 |
| 5.1 | Polygon | 151 |
| 5.2 | Konvexe Hülle..... | 158 |
| 5.3 | Graham-Scan-Algorithmus..... | 163 |
| 5.4 | Jarvis-March-Algorithmus | 167 |
| 5.5 | Quickhull-Algorithmus..... | 170 |
| 5.6 | Aufgaben | 175 |
| 6 | Codierung | 177 |
| 6.1 | Huffman-Code..... | 179 |
| 6.2 | CRC-Verfahren..... | 184 |
| 6.3 | Aufgaben | 191 |

| | | |
|-----------|---|------------|
| 7 | Kryptografie | 193 |
| 7.1 | RSA-Verschlüsselung | 194 |
| 7.2 | Zahlentheoretische Grundlagen | 197 |
| 7.3 | Modulare Exponentiation | 204 |
| 7.4 | Erweiterter euklidischer Algorithmus | 206 |
| 7.5 | Primzahltest | 208 |
| 7.6 | Chinesischer Restsatz | 212 |
| 7.7 | Quadratisches Sieb | 215 |
| 7.8 | Diffie-Hellman-Schlüsselvereinbarung | 219 |
| 7.9 | ElGamal-Verschlüsselung | 221 |
| 7.10 | Elliptische Kurven | 225 |
| 7.11 | Diffie-Hellman-Schlüsselvereinbarung mit elliptischer Kurve | 230 |
| 7.12 | Aufgaben | 231 |
| 8 | Arithmetik | 233 |
| 8.1 | Ripple-Carry-Addierer | 233 |
| 8.2 | Carry-Lookahead-Addierer | 235 |
| 8.3 | Carry-Save-Addierer | 239 |
| 8.4 | Modulare Multiplikation | 240 |
| 9 | Transformationen | 247 |
| 9.1 | Transformation von Polynomen | 250 |
| 9.2 | Schnelle Fouriertransformation (FFT) | 254 |
| 9.3 | Diskrete Kosinustransformation | 262 |
| 9.4 | Aufgaben | 265 |
| 10 | NP-vollständige Probleme | 267 |
| 10.1 | Effizient lösbare Probleme | 267 |
| 10.2 | Reduktion von Problemen | 267 |
| 10.3 | Die Mengen P und NP | 270 |
| 10.4 | NP-Vollständigkeit | 273 |
| 10.5 | Aufgaben | 276 |

| | | |
|-----------|--|------------|
| 11 | Formale Verifikation | 277 |
| 11.1 | Semantikregeln | 277 |
| 11.2 | Korrektheit von If-Else-Anweisungen | 281 |
| 11.3 | Korrektheit von While-Schleifen | 283 |
| 11.4 | Totale Korrektheit von While-Schleifen | 285 |
| 11.5 | Zusammenfassung | 290 |
| 11.6 | Aufgaben | 291 |
| 12 | Sortiernetze | 293 |
| 12.1 | Vergleichernetze | 293 |
| 12.2 | 0-1-Prinzip | 296 |
| 12.3 | Bubblesort | 298 |
| 12.4 | Odd-even Transposition Sort | 300 |
| 12.5 | Bitonic Sort | 302 |
| 12.6 | Odd-even Mergesort | 309 |
| 12.7 | Shellsort | 314 |
| 13 | Sortieren auf Prozessorfeldern | 317 |
| 13.1 | LS3-Sort | 320 |
| 13.2 | $3n$ -Sort | 323 |
| A | Mathematische Grundlagen | 329 |
| A.1 | Menge, Relation, Abbildung | 329 |
| A.2 | Graph | 341 |
| A.3 | Metrik | 347 |
| A.4 | Gruppe | 349 |
| A.5 | Ring, Körper | 355 |
| A.6 | Vektorraum | 358 |
| A.7 | Teilbarkeit, Kongruenz modulo n | 364 |
| A.8 | Asymptotische Komplexität | 368 |

| | | |
|--------------|-----------------------------------|------------|
| B | Java-Programmierkonstrukte | 373 |
| B.1 | Interface | 373 |
| B.2 | Typ-Parameter | 374 |
| B.3 | Iterator | 376 |
| C | Literaturverzeichnis | 381 |
| Index | | 387 |