

# Contents

|   |     |
|---|-----|
| <i>Preface</i>                                | vii |
| 1. Preliminaries                              | 1   |
| 1.1 Induction . . . . .                       | 1   |
| 1.2 Invariance . . . . .                      | 4   |
| 1.3 Correctness of algorithms . . . . .       | 5   |
| 1.3.1 Division algorithm . . . . .            | 6   |
| 1.3.2 Euclid's algorithm . . . . .            | 7   |
| 1.3.3 Palindromes algorithm . . . . .         | 8   |
| 1.3.4 Further examples . . . . .              | 9   |
| 1.3.5 Recursion and fixed points . . . . .    | 12  |
| 1.4 Stable marriage . . . . .                 | 14  |
| 1.5 Answers to selected problems . . . . .    | 17  |
| 1.6 Notes . . . . .                           | 27  |
| 2. Greedy Algorithms                          | 29  |
| 2.1 Minimum cost spanning trees . . . . .     | 29  |
| 2.2 Jobs with deadlines and profits . . . . . | 34  |
| 2.3 Further examples and problems . . . . .   | 36  |
| 2.3.1 Make change . . . . .                   | 36  |
| 2.3.2 Maximum weight matching . . . . .       | 37  |
| 2.3.3 Shortest path . . . . .                 | 38  |
| 2.4 Answers to selected problems . . . . .    | 38  |
| 2.5 Notes . . . . .                           | 42  |

|       |  |     |
|-------|--|-----|
| 3.    | Divide and Conquer                                   | 43  |
| 3.1   | Mergesort . . . . .                                  | 44  |
| 3.2   | Multiplying numbers in binary . . . . .              | 45  |
| 3.3   | Savitch's algorithm . . . . .                        | 48  |
| 3.4   | Answers to selected problems . . . . .               | 49  |
| 3.5   | Notes . . . . .                                      | 50  |
| 4.    | Dynamic Programming                                  | 51  |
| 4.1   | Longest monotone subsequence problem . . . . .       | 51  |
| 4.2   | All pairs shortest path problem . . . . .            | 52  |
| 4.3   | Simple knapsack problem . . . . .                    | 54  |
| 4.3.1 | Dispersed knapsack . . . . .                         | 58  |
| 4.4   | General knapsack problem . . . . .                   | 58  |
| 4.5   | Activity selection problem . . . . .                 | 59  |
| 4.6   | Jobs with deadlines, durations and profits . . . . . | 62  |
| 4.7   | Further examples and problems . . . . .              | 63  |
| 4.7.1 | Consecutive subsequence sum problem . . . . .        | 63  |
| 4.7.2 | Context free grammars . . . . .                      | 64  |
| 4.8   | Answers to selected problems . . . . .               | 67  |
| 4.9   | Notes . . . . .                                      | 71  |
| 5.    | Online Algorithms                                    | 73  |
| 5.1   | List accessing problem . . . . .                     | 74  |
| 5.2   | Paging . . . . .                                     | 78  |
| 5.2.1 | Demand paging . . . . .                              | 79  |
| 5.2.2 | FIFO . . . . .                                       | 82  |
| 5.2.3 | LRU . . . . .  | 82  |
| 5.2.4 | Marking algorithms . . . . .                         | 86  |
| 5.2.5 | FWF . . . . .  | 87  |
| 5.2.6 | LFD . . . . .  | 88  |
| 5.3   | Answers to selected problems . . . . .               | 92  |
| 5.4   | Notes . . . . .                                      | 94  |
| 6.    | Randomized Algorithms                                | 95  |
| 6.1   | Perfect matching . . . . .                           | 96  |
| 6.2   | Pattern matching . . . . .                           | 100 |
| 6.3   | Primality testing . . . . .                          | 101 |
| 6.4   | Public key cryptography . . . . .                    | 105 |

|   |  |     |
|---|--|-----|
| 6.4.1                                     | Diffie-Hellman key exchange . . . . .  | 106 |
| 6.4.2                                     | ElGamal . . . . .                      | 107 |
| 6.4.3                                     | RSA . . . . .                          | 107 |
| 6.5                                       | Answers to selected problems . . . . . | 109 |
| 6.6                                       | Notes . . . . .                        | 111 |
| Appendix A Number Theory and Group Theory |  | 113 |
| A.1                                       | Answers to selected problems . . . . . | 118 |
| A.2                                       | Notes . . . . .                        | 118 |
| Appendix B Relations                      |  | 119 |
| B.1                                       | Closure . . . . .                      | 120 |
| B.2                                       | Equivalence relation . . . . .         | 121 |
| B.3                                       | Partial orders . . . . .               | 123 |
| B.4                                       | Lattices . . . . .                     | 124 |
| B.5                                       | Fixed point theory . . . . .           | 125 |
| B.6                                       | Answers to selected problems . . . . . | 128 |
| B.7                                       | Notes . . . . .                        | 128 |
| <i>Bibliography</i>                       |  | 129 |
| <i>Index</i>                              |  | 131 |