

contents

1 what's it all about? 1

Algorithms 2

Basic instructions 5

The text vs. the process 7

Inputs 9

What do algorithms solve? 10

Isn't our setup too simplistic? 15

Solving algorithmic problems 16

Programming 18

Errors and correctness 21

Termination 26

2 sometimes we can't do it 27

Finite problems are solvable 29

The tiling problem 30

Do we really mean it? 33

Elementary computing devices 36

The Church–Turing thesis 40

Computability is robust 42

Domino snakes 46

Program verification 48

The halting problem 50

Nothing about computation can be computed! 53

Some problems are even worse 54

- 3 sometimes we can't afford to do it 59
 - Resources: time and memory space 60
 - Improving running time 61
 - Upper and lower bounds 65
 - So what? 69
 - The towers of Hanoi 69
 - The good, the bad, and the ugly 73
 - Intractability 78
 - Roadblocks and chess 82
 - Problems that are even harder 85
 - Unreasonable memory requirements 88

- 4 Sometimes we just don't know 91
 - The monkey puzzle 92
 - NP-complete problems 95
 - Finding short paths 97
 - Scheduling and matching 100
 - More on puzzles 102
 - Coloring networks 104
 - Magic coins 106
 - Standing or falling together 109
 - The great mystery: is P equal to NP? 111
 - Can we come close? 113
 - Sometimes we succeed 115

- 5 Trying to ease the pain 119
 - Parallelism, or joining forces 121
 - Can parallelism eliminate the bad news? 124
 - Randomization, or tossing coins 129
 - More on Monte Carlo algorithms 132
 - Testing for primality 134

Randomized primality testing 136
 Can randomization eliminate the bad news? 140
 Can computers simulate true randomness? 141
 Quantum computing 143
 Quantum algorithms 146
 Can there be a quantum computer? 151
 Molecular computing 153

6 Turning bad into good 157

Classical cryptography 158
 Public-key cryptography 161
 Signing messages 165
 Can this be made to work? 168
 The RSA cryptosystem 170
 Interactive proofs 173
 Zero-knowledge proofs 177
 I can 3-color a network 180
 On millionaires, ballots, and more 186

7 Can we ourselves do any better? 189

Algorithmic intelligence? 191
 The Turing test 192
 ELIZA and zupchoks 196
 Heuristics 199
 What is knowledge? 204
 Understanding natural language 208

Postamble 213

Index 215