
Contents

Part I Foundations of Computer Science

1	Compressing and Correcting Digital Media	3
1.1	A Compact Disk = a Sequence of Numbers	5
1.1.1	Decimal and Binary Representation	6
1.1.2	Decimal and Binary Notation	9
1.1.3	Grouping Bits into Bytes	10
1.2	Data Compression	11
1.2.1	A Run-Length Based Approach	13
1.2.2	A Dictionary-Based Approach	15
1.3	Error Correction	18
1.3.1	An Error Detection Approach	18
1.3.2	An Error Correction Approach	21
1.4	Recasting Error Correction as Matrix Arithmetic	23
1.4.1	An Overview of Vectors	24
1.4.2	An Overview of Matrices	25
1.4.3	Addition and Multiplication Modulo 2	27
1.4.4	Using Matrices for Error Correction	28
1.4.5	Generalising the Matrix-Based (7, 4)-Code	31
	References	31
2	Writing and Comparing Algorithms	33
2.1	Algorithms	33
2.1.1	What Is an Algorithm?	34
2.1.2	What Is not an Algorithm?	37
2.2	Algorithms for Multiplication	38
2.3	Algorithms for Exponentiation	42
2.4	Computational Complexity	44
2.4.1	Step Counting and Dominant Steps	45
2.4.2	Problem Size and Step Counting Functions	46

2.4.3	Ignoring Small Problems and Minor Terms	47
2.4.4	Studying the Growth of Functions	49
	References	51
3	Playing Hide-and-Seek with Virus Scanners	53
3.1	Computers and Programs	55
3.1.1	A Theoretical Computer	56
3.1.2	A Real, Harvard-Style Computer	57
3.1.3	A Real, von Neumann-Style Computer	59
3.2	Harvard Versus von Neumann Computers	66
3.2.1	Beyond Straight-Line Programs	67
3.2.2	Toward Self-Modifying Programs	68
3.3	A Self-Modifying Virus	70
3.3.1	Using XOR to Mask Numbers	70
3.3.2	A Virus that Masks the Payload	71
3.3.3	Preventing the Virus Without a Virus Scanner	73
	References	74
4	How Long Is a Piece of String?	77
4.1	String Data Structures	78
4.1.1	Problem #1: Representing Characters	80
4.1.2	Problem #2: Representing Strings	82
4.2	String Algorithms	84
4.2.1	strlen: Finding the Length of a String	84
4.2.2	toupper: Converting a String to Upper-Case	86
4.2.3	strcmp: Testing if One String Is the Same as Another	89
4.2.4	strcat: Concatenating Two Strings Together	91
4.2.5	Problem #3: Repeated Concatenation	95
	References	97
5	Demystifying Web-Search: the Mathematics of PageRank	99
5.1	PageRank: the Essence of Google Web-Search	100
5.1.1	What Actually <i>Is</i> Web-Search?	100
5.1.2	Web-Search Before Google	101
5.1.3	Web-Search After Google	102
5.2	Using Graph Theory to Model and Explore the Web	103
5.2.1	Graph Traversal	105
5.2.2	Graph Exploration	109
5.3	Using Probability Theory to Model Web-Browsing	110
5.3.1	Sanitising the Web-Graph to Avoid a Subtle Problems	113
5.3.2	A Mathematical Approach to Computing PageRank	114
5.4	Putting It All Together: Using PageRank to Produce Web-Search Results	121
	References	123

Part II Examples from Information Security

6	Using Short Programs to Make and Break Historical Ciphers . . .	127
6.1	Shift Ciphers	128
6.1.1	Encryption and Decryption	128
6.1.2	Cryptanalysis	135
6.2	Substitution Ciphers	138
6.2.1	Encryption and Decryption	139
6.2.2	Cryptanalysis	141
	References	147
7	Generation and Testing of Random Numbers	149
7.1	What <i>Is</i> Randomness?	150
7.1.1	Biased Versus Unbiased	151
7.1.2	Predictable Versus Unpredictable	152
7.1.3	Random Versus Arbitrary	153
7.2	Real Randomness	154
7.2.1	Generating Randomness	154
7.2.2	Testing Randomness	155
7.3	Fake Randomness	159
7.3.1	Generating Randomness	159
7.3.2	Testing Randomness	164
	References	167
8	Safety in Numbers: Modern Cryptography from Ancient Arithmetic	169
8.1	Modular Arithmetic: the Theory	171
8.1.1	Rules for Modular Addition	172
8.1.2	Rules for Modular Multiplication	173
8.1.3	The Sets \mathbb{Z} , \mathbb{Z}_N and \mathbb{Z}_N^*	175
8.1.4	Some Interesting Facts About \mathbb{Z}_N^*	177
8.2	Modular Arithmetic: the Practice	179
8.2.1	Addition and Subtraction	179
8.2.2	Multiplication	181
8.2.3	Exponentiation	183
8.2.4	Division (via Inversion)	183
8.3	From Modular Arithmetic to Cryptographic Protocols	190
8.3.1	Diffie-Hellman Key Exchange	190
8.3.2	RSA Encryption	192
8.3.3	Functional Versus Secure	194
	References	197

9	Hiding a Needle in a Haystack: Concealed Messages	199
9.1	Digital Images	200
9.1.1	Rasterised Images	200
9.1.2	Vector Images	204
9.2	Steganography	208
9.2.1	Rasterised Images: “Stolen LSBs”	208
9.2.2	Vector Images: “Microdots”	211
	References	212
10	Picking Digital Pockets	215
10.1	Passive Physical Attacks	217
10.1.1	Attack	217
10.1.2	Countermeasures	221
10.2	Active Physical Attacks	224
10.2.1	Attack	224
10.2.2	Countermeasures	225
	References	227
	Index	229

What Is Computer Science?

An Information Security Perspective

Page, D.; Smart, N.

2014, XVIII, 232 p. 84 illus., Softcover

ISBN: 978-3-319-04041-7