

Mathematics for Computer Science

revised Wednesday 8th September, 2010, 00:40

Eric Lehman

Google Inc.

F Thomson Leighton

Department of Mathematics and CSAIL, MIT

Akamai Technologies

Albert R Meyer










Massachusetts Institute of Technology

Contents






I Proofs

1	Propositions	5
1.1	Compound Propositions	6
1.2	Propositional Logic in Computer Programs	10
1.3	Predicates and Quantifiers	11
1.4	Validity	19
1.5	Satisfiability	21
2	Patterns of Proof	23
2.1	The Axiomatic Method	23
2.2	Proof by Cases	26
2.3	Proving an Implication	27
2.4	Proving an “If and Only If”	30
2.5	Proof by Contradiction	32
2.6	Proofs about Sets	33
2.7	Good Proofs in Practice	40
3	Induction	43
3.1	The Well Ordering Principle	43
3.2	Ordinary Induction	46
3.3	Invariants	56
3.4	Strong Induction	64
3.5	Structural Induction	69
4	Number Theory	81
4.1	Divisibility	81
4.2	The Greatest Common Divisor	87
4.3	The Fundamental Theorem of Arithmetic	94
4.4	Alan Turing	96
4.5	Modular Arithmetic	100
4.6	Arithmetic with a Prime Modulus	103
4.7	Arithmetic with an Arbitrary Modulus	108
4.8	The RSA Algorithm	113

II Structures

- 5 Graph Theory 121**
 -  Definitions 121
 -  Matching Problems 128
 -  Coloring 143
 - 5.4 Getting from A to B in a Graph 147
 - 5.5 Connectivity 151
 - 5.6 Around and Around We Go 156
 - 5.7 Trees 162
 - 5.8 Planar Graphs 170
- 6 Directed Graphs 189**
 -  Definitions 189
 - 6.2 Tournament Graphs 192
 -  Communication Networks 196
- 7 Relations and Partial Orders 213**
 -  Binary Relations 213
 - 7.2 Relations and Cardinality 217
 -  Relations on One Set 220
 -  Equivalence Relations 222
 - 7.5 Partial Orders 225
 - 7.6 Posets and DAGs 226
 - 7.7 Topological Sort 229
 -  Parallel Task Scheduling 232
 - 7.9 Dilworth’s Lemma 235
- 8 State Machines 237**

III Counting

- 9 Sums and Asymptotics 243**
 -  The Value of an Annuity 244
 -  Power Sums 250
 -  Approximating Sums 252
 - 9.4 Hanging Out Over the Edge 257
 -  Double Trouble 269
 -  Products 272

	9 Asymptotic Notation	275
10	Recurrences	283
10.1	The Towers of Hanoi	284
10.2	Merge Sort	291
10.3	Linear Recurrences	294
10.4	Divide-and-Conquer Recurrences	302
10.5	A Feel for Recurrences	309
11	Cardinality Rules	313
11.1	Counting One Thing by Counting Another	313
11.2	Counting Sequences	314
11.3	The Generalized Product Rule	317
11.4	The Division Rule	321
11.5	Counting Subsets	324
11.6	Sequences with Repetitions	326
11.7	Counting Practice: Poker Hands	329
11.8	Inclusion-Exclusion	334
11.9	Combinatorial Proofs	339
11.10	The Pigeonhole Principle	342
11.11	A Magic Trick	346
12	Generating Functions	355
12.1	Definitions and Examples	355
12.2	Operations on Generating Functions	356
12.3	Evaluating Sums	361
12.4	Extracting Coefficients	363
12.5	Solving Linear Recurrences	370
12.6	Counting with Generating Functions	374
13	Infinite Sets	379
13.1	Injections, Surjections, and Bijections	379
13.2	Countable Sets	381
13.3	Power Sets Are Strictly Bigger	384
13.4	Infinites in Computer Science	386

IV Probability

14	Events and Probability Spaces	391
14.1	Let’s Make a Deal	391
14.2	The Four Step Method	392

14.3	Strange Dice	402
14.4	Set Theory and Probability	411
14.5	Infinite Probability Spaces	413
15	Conditional Probability	417
15.1	Definition	417
15.2	Using the Four-Step Method to Determine Conditional Probability	418
15.3	<i>A Posteriori</i> Probabilities	424
15.4	Conditional Identities	427
16	Independence	431
16.1	Definitions	431
16.2	Independence Is an Assumption	432
16.3	Mutual Independence	433
16.4	Pairwise Independence	435
16.5	The Birthday Paradox	438
17	Random Variables and Distributions	445
17.1	Definitions and Examples	445
17.2	Distribution Functions	450
17.3	Bernoulli Distributions	452
17.4	Uniform Distributions	453
17.5	Binomial Distributions	456
18	Expectation	467
18.1	Definitions and Examples	467
18.2	Expected Returns in Gambling Games	477
18.3	Expectations of Sums	483
18.4	Expectations of Products	490
18.5	Expectations of Quotients	492
19	Deviations	497
19.1	Variance	497
19.2	Markov’s Theorem	507
19.3	Chebyshev’s Theorem	513
19.4	Bounds for Sums of Random Variables	516
19.5	Mutually Independent Events	523
20	Random Walks	533
20.1	Unbiased Random Walks	533
20.2	Gambler’s Ruin	542
20.3	Walking in Circles	549