Contents

Preface

1 Events and Probability
   1.1 Application: Verifying Polynomial Identities 1
   1.2 Axioms of Probability 3
   1.3 Application: Verifying Matrix Multiplication 8
   1.4 Application: A Randomized Min-Cut Algorithm 12
   1.5 Exercises 14

2 Discrete Random Variables and Expectation
   2.1 Random Variables and Expectation 20
      2.1.1 Linearity of Expectations 22
      2.1.2 Jensen’s Inequality 23
   2.2 The Bernoulli and Binomial Random Variables 25
   2.3 Conditional Expectation 26
   2.4 The Geometric Distribution 30
      2.4.1 Example: Coupon Collector’s Problem 32
   2.5 Application: The Expected Run-Time of Quicksort 34
   2.6 Exercises 38

3 Moments and Deviations
   3.1 Markov’s Inequality 44
   3.2 Variance and Moments of a Random Variable 45
      3.2.1 Example: Variance of a Binomial Random Variable 48
   3.3 Chebyshev’s Inequality 48
      3.3.1 Example: Coupon Collector’s Problem 50
   3.4 Application: A Randomized Algorithm for Computing the Median 52
      3.4.1 The Algorithm 53
      3.4.2 Analysis of the Algorithm 54
   3.5 Exercises 57
CONTENTS

4 Chernoff Bounds 61
  4.1 Moment Generating Functions 61
  4.2 Deriving and Applying Chernoff Bounds 63
    4.2.1 Chernoff Bounds for the Sum of Poisson Trials 63
    4.2.2 Example: Coin Flips 67
    4.2.3 Application: Estimating a Parameter 67
  4.3 Better Bounds for Some Special Cases 69
  4.4 Application: Set Balancing 71
  4.5* Application: Packet Routing in Sparse Networks 72
    4.5.1 Permutation Routing on the Hypercube 73
    4.5.2 Permutation Routing on the Butterfly 78
  4.6 Exercises 83

5 Balls, Bins, and Random Graphs 90
  5.1 Example: The Birthday Paradox 90
  5.2 Balls into Bins 92
    5.2.1 The Balls-and-Bins Model 92
    5.2.2 Application: Bucket Sort 93
  5.3 The Poisson Distribution 94
    5.3.1 Limit of the Binomial Distribution 98
  5.4 The Poisson Approximation 99
    5.4.1* Example: Coupon Collector’s Problem, Revisited 104
  5.5 Application: Hashing 106
    5.5.1 Chain Hashing 106
    5.5.2 Hashing: Bit Strings 108
    5.5.3 Bloom Filters 109
    5.5.4 Breaking Symmetry 112
  5.6 Random Graphs 112
    5.6.1 Random Graph Models 112
    5.6.2 Application: Hamiltonian Cycles in Random Graphs 113
  5.7 Exercises 118
  5.8 An Exploratory Assignment 124

6 The Probabilistic Method 126
  6.1 The Basic Counting Argument 126
  6.2 The Expectation Argument 128
    6.2.1 Application: Finding a Large Cut 129
    6.2.2 Application: Maximum Satisfiability 130
  6.3 Derandomization Using Conditional Expectations 131
  6.4 Sample and Modify 133
    6.4.1 Application: Independent Sets 133
    6.4.2 Application: Graphs with Large Girth 134
  6.5 The Second Moment Method 134
    6.5.1 Application: Threshold Behavior in Random Graphs 135
## CONTENTS

6.6 The Conditional Expectation Inequality 136
6.7 The Lovasz Local Lemma 138
  6.7.1 Application: Edge-Disjoint Paths 141
  6.7.2 Application: Satisfiability 142
6.8* Explicit Constructions Using the Local Lemma 142
  6.8.1 Application: A Satisfiability Algorithm 143
6.9 Lovasz Local Lemma: The General Case 146
6.10 Exercises 148

7 Markov Chains and Random Walks 153
  7.1 Markov Chains: Definitions and Representations 153
    7.1.1 Application: A Randomized Algorithm for 2-Satisfiability 156
    7.1.2 Application: A Randomized Algorithm for 3-Satisfiability 159
  7.2 Classification of States 163
    7.2.1 Example: The Gambler’s Ruin 166
  7.3 Stationary Distributions 167
    7.3.1 Example: A Simple Queue 173
  7.4 Random Walks on Undirected Graphs 174
    7.4.1 Application: An s–t Connectivity Algorithm 176
  7.5 Parrondo’s Paradox 177
  7.6 Exercises 182

8 Continuous Distributions and the Poisson Process 188
  8.1 Continuous Random Variables 188
    8.1.1 Probability Distributions in ℝ 188
    8.1.2 Joint Distributions and Conditional Probability 191
  8.2 The Uniform Distribution 193
    8.2.1 Additional Properties of the Uniform Distribution 194
  8.3 The Exponential Distribution 196
    8.3.1 Additional Properties of the Exponential Distribution 197
    8.3.2* Example: Balls and Bins with Feedback 199
  8.4 The Poisson Process 201
    8.4.1 Interarrival Distribution 204
    8.4.2 Combining and Splitting Poisson Processes 205
    8.4.3 Conditional Arrival Time Distribution 207
  8.5 Continuous Time Markov Processes 210
  8.6 Example: Markovian Queues 212
    8.6.1 M/M/1 Queue in Equilibrium 213
    8.6.2 M/M/1/K Queue in Equilibrium 216
    8.6.3 The Number of Customers in an M/M/∞ Queue 216
  8.7 Exercises 219

9 Entropy, Randomness, and Information 225
  9.1 The Entropy Function 225
  9.2 Entropy and Binomial Coefficients 228
## CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.3</td>
<td>Entropy: A Measure of Randomness</td>
<td>230</td>
</tr>
<tr>
<td>9.4</td>
<td>Compression</td>
<td>234</td>
</tr>
<tr>
<td>9.5*</td>
<td>Coding: Shannon’s Theorem</td>
<td>237</td>
</tr>
<tr>
<td>9.6</td>
<td>Exercises</td>
<td>245</td>
</tr>
<tr>
<td>10</td>
<td>The Monte Carlo Method</td>
<td>252</td>
</tr>
<tr>
<td>10.1</td>
<td>The Monte Carlo Method</td>
<td>252</td>
</tr>
<tr>
<td>10.2</td>
<td>Application: The DNF Counting Problem</td>
<td>255</td>
</tr>
<tr>
<td>10.2.1</td>
<td>The Naïve Approach</td>
<td>255</td>
</tr>
<tr>
<td>10.2.2</td>
<td>A Fully Polynomial Randomized Scheme for DNF Counting</td>
<td>257</td>
</tr>
<tr>
<td>10.3</td>
<td>From Approximate Sampling to Approximate Counting</td>
<td>259</td>
</tr>
<tr>
<td>10.4</td>
<td>The Markov Chain Monte Carlo Method</td>
<td>263</td>
</tr>
<tr>
<td>10.4.1</td>
<td>The Metropolis Algorithm</td>
<td>265</td>
</tr>
<tr>
<td>10.5</td>
<td>Exercises</td>
<td>267</td>
</tr>
<tr>
<td>10.6</td>
<td>An Exploratory Assignment on Minimum Spanning Trees</td>
<td>270</td>
</tr>
<tr>
<td>11*</td>
<td>Coupling of Markov Chains</td>
<td>271</td>
</tr>
<tr>
<td>11.1</td>
<td>Variation Distance and Mixing Time</td>
<td>271</td>
</tr>
<tr>
<td>11.2</td>
<td>Coupling</td>
<td>274</td>
</tr>
<tr>
<td>11.2.1</td>
<td>Example: Shuffling Cards</td>
<td>275</td>
</tr>
<tr>
<td>11.2.2</td>
<td>Example: Random Walks on the Hypercube</td>
<td>276</td>
</tr>
<tr>
<td>11.2.3</td>
<td>Example: Independent Sets of Fixed Size</td>
<td>277</td>
</tr>
<tr>
<td>11.3</td>
<td>Application: Variation Distance Is Nonincreasing</td>
<td>278</td>
</tr>
<tr>
<td>11.4</td>
<td>Geometric Convergence</td>
<td>281</td>
</tr>
<tr>
<td>11.5</td>
<td>Application: Approximately Sampling Proper Colorings</td>
<td>282</td>
</tr>
<tr>
<td>11.6</td>
<td>Path Coupling</td>
<td>286</td>
</tr>
<tr>
<td>11.7</td>
<td>Exercises</td>
<td>289</td>
</tr>
<tr>
<td>12</td>
<td>Martingales</td>
<td>295</td>
</tr>
<tr>
<td>12.1</td>
<td>Martingales</td>
<td>295</td>
</tr>
<tr>
<td>12.2</td>
<td>Stopping Times</td>
<td>297</td>
</tr>
<tr>
<td>12.2.1</td>
<td>Example: A Ballot Theorem</td>
<td>299</td>
</tr>
<tr>
<td>12.3</td>
<td>Wald’s Equation</td>
<td>300</td>
</tr>
<tr>
<td>12.4</td>
<td>Tail Inequalities for Martingales</td>
<td>303</td>
</tr>
<tr>
<td>12.5</td>
<td>Applications of the Azuma–Hoeffding Inequality</td>
<td>305</td>
</tr>
<tr>
<td>12.5.1</td>
<td>General Formalization</td>
<td>305</td>
</tr>
<tr>
<td>12.5.2</td>
<td>Application: Pattern Matching</td>
<td>307</td>
</tr>
<tr>
<td>12.5.3</td>
<td>Application: Balls and Bins</td>
<td>308</td>
</tr>
<tr>
<td>12.5.4</td>
<td>Application: Chromatic Number</td>
<td>308</td>
</tr>
<tr>
<td>12.6</td>
<td>Exercises</td>
<td>309</td>
</tr>
<tr>
<td>13</td>
<td>Pairwise Independence and Universal Hash Functions</td>
<td>314</td>
</tr>
<tr>
<td>13.1</td>
<td>Pairwise Independence</td>
<td>314</td>
</tr>
<tr>
<td>13.1.1</td>
<td>Example: A Construction of Pairwise Independent Bits</td>
<td>315</td>
</tr>
<tr>
<td>13.1.2</td>
<td>Application: Derandomizing an Algorithm for Large Cuts</td>
<td>316</td>
</tr>
</tbody>
</table>