Contents

Preface xiii

About the Author xix

Dependency Chart xxi

Chapter 1: Logic and Sets 1

1.1: Logical Operators: Statements and Truth Values, Negations, Conjunctions, and Disjunctions, Truth Tables, Conditional Statements (Implications), Converses and Contrapositives, Logical Equivalence and Biconditionals, Hierarchy of Logical Operators, Some Useful Logical Equivalences, Logical Implication, Proofs and Counterexamples, Logical Puzzles, Exercises, Computer Exercises

1.2: Logical Quantifiers: Predicates and Universes, Universal and Existential Quantifiers, Negations of Quantifiers, Nested Quantifiers, Exercises

1.3: Sets: Sets and Their Elements, Unions and Intersections, Venn Diagrams, Subsets and the Empty Set, Complements and Differences of Sets, Set Theoretic Identities, Unions and Intersections of Set Families, Power Sets, Cartesian Products of Sets, The Historical Development of Logic and Sets, Exercises, Computer Exercises

Chapter 2: Relations and Functions, Boolean Algebra, and Circuit Design 61

2.1: Relations and Functions: Binary Relations, Functions, Function Images and Pre-images, One-to-One, Onto, and Bijective Functions, Inverse Functions, Exercises

2.2: Equivalence Relations and Partial Orderings: Equivalence Relations, Congruence Modulo a Positive Integer, Equivalence Classes and Their Representatives, Strings, Partial Order(ings), Hasse Diagrams, Poset Isomorphisms, Exercises

2.3: Boolean Algebra and Circuit Design: Boolean Operations, Variables, and Functions, Boolean Algebra Identities, Sums, Products, and Complements of Boolean Functions, Sums of Products Expansions (Disjunctive Normal Form), Duality, Logic Gates and Circuit Designs, Karnaugh Maps, Exercises

Chapter 3: The Integers, Induction, and Recursion 111

3.1: Mathematical Induction: The Principle of Mathematical Induction: Basic Form, The Principle of Mathematical Induction: General Form, Strong Mathematical Induction, Finite Geometric Series, Exercises

3.2: Recursion: Infinite Sequences, Recursion and Recursively Defined Sequences, The Fibonacci Sequence, Recursive Sequences of Higher Degree, Explicit Solution Methods for Linear Recursion Formulas, Exercises

Appendix: Recursive Definitions and Structural Induction

Computer Exercises

3.3: Some Topics in Elementary Number Theory: Divisibility, Primes, The Prime Number Theorem, Greatest Common Divisors, Relatively Prime Integers, The Division Algorithm, The Euclidean Algorithm, Congruent Substitutions in Modular Arithmetic, Fermat's Little Theorem, Euler's Theorem, Orders and Primitive Roots, Exercises, Computer Exercises

Appendix: Probabilistic Primality Tests

Chapter 4: Number Systems 187

4.1: Representations of Integers in Different Bases: Representation of Integers in a Base *b*, Hex(adecimal) and Binary Expansions, Addition Algorithm with Base *b* Expansions, Subtraction Algorithm with Base *b* Expansions, Multiplication Algorithm in Base *b* Expansions, Exercises, Computer Exercises

4.2: Modular Arithmetic and Congruences: Modular Integer Systems, Modular Inverses, Fast Modular Exponentiation, Congruences, The Extended Euclidean Algorithm, Solving Linear Congruences, The Chinese Remainder Theorem, Pseudo-Random Numbers: The Linear Congruential Method, Exercises, Computer Exercises

4.3: Matrices: Matrix Addition, Subtraction, and Scalar Multiplication, Matrix Multiplication, Matrix Arithmetic, Definition of an Invertible

(Square) Matrix, The Determinant of a Square Matrix, Inverses of 2 × 2 Matrices, The Transpose of a Matrix, Modular Integer Matrices, The Classical Adjoint (for Matrix Inversions), Application of Modular Matrices: The Hill Cryptosystem, Exercises, Computer Exercises

4.4: Floating Point Arithmetic: Exact Arithmetic, Floating Point Arithmetic Systems, Unit Roundoff (Machine Epsilon), Underflows, Overflows, Exercises, Computer Exercises

4.5: Public Key Cryptography: An Informal Analogy for a Public Key Cryptosystem, The Quest for Secure Electronic Key Exchange, One-Way Functions, Review of the Discrete Logarithm Problem, The Diffie–Hellman Key Exchange, The Quest for a Complete Public Key Cryptosystem, The RSA Cryptosystem, The El Gamal Cryptosystem, Knapsack Problems, The Merkle–Hellman Knapsack Cryptosystem, Government Controls on Cryptography, Exercises, Computer Exercises

Chapter 5: Counting Techniques, Combinatorics, and Generating Functions 311

5.1: Fundamental Principles of Counting: The Multiplication Principle, the Complement Principle, The Inclusion-Exclusion Principle, The Pigeonhole Principle, The Generalized Pigeonhole Principle, Exercises

5.2: Permutations, Combinations, and the Binomial Theorem: The Difference between a Permutation and a Combination, Computing and Counting with Permutations and Combinations, the Binomial Theorem, Multinomial Coefficients, The Multinomial Theorem, Exercises

5.3: Generating Functions: Generating Functions and Power Series, Arithmetic of Generating Functions, The Generalized Binomial Theorem, Using Generating Functions to Solve Recursive Sequences, Using Generating Functions in Counting Problems, Exercises

Appendix: Application to Weighted Democracies

Computer Exercises

Chapter 6: Discrete Probability and Simulation 379

6.1: Introduction To Discrete Probability: Experiments, Sample Spaces, and Events, Experiments with Equally Likely Outcomes, Kolmogorov's Axioms, Probability Rules, Conditional Probability, The Multiplication Rule, Conditioning and Bayes' Formula, Independent Events, Discrete Problems with Infinite Sample Spaces, Exercises

6.2: Random Numbers, Random Variables, and Basic Simulations: Probabilities as Relative Frequencies, Random Numbers and Random Variables, Binomial Random Variables, Continuous Random Variables, Uniform Random Variables, Setting up a Simulation, Generating Random Permutations and Random Subsets, Expectation and Variance of a Random Variable, Independence of Random Variables, Linearity of Expectation, Properties of Variances, Poisson Random Variables, Exercises, Computer Exercises

Chapter 7: Complexity of Algorithms 449

7.1: Some Algorithms for Searching and Sorting: The Linear Search Algorithm, The Binary Search Algorithm, The Selection Sort Algorithm, the Bubble Sort Algorithm, The Quick Sort Algorithm, The Merge Sort Algorithm, A Randomized Algorithm for Computing Medians, Exercises, Computer Exercises

7.2: Growth Rates of Functions and the Complexity of Algorithms: A Brief and Informal Preview, Big-O Notation, Combinations of Big-O Estimates, Big-Omega and Big-Theta Notation, Complexity of Algorithms, Optimality of the Merge Sort Algorithm, the Classes *P* and *NP*, Exercises, Computer Exercises

Chapter 8: Graphs, Trees, and Associated Algorithms 495

8.1: Graph Concepts and Properties: Simple Graphs, General Graphs, Degrees, Regular Graphs, and the Handshaking Theorem, Some Important Families of Simple Graphs, Bipartite Graphs, Degree Sequences, Subgraphs, Isomorphism of Simple Graphs, the Complement of a Simple Graph, Representing Graphs on Computers, Directed Graphs (Digraphs), Some Graph Models for Optimization Problems, Exercises, Computer Exercises

8.2: Paths, Connectedness, and Distances in Graphs: Paths, Circuits and Reachability in Graphs, Paths, Circuits, and Reachability in Digraphs, Connectedness and Connected Components, Distances and Diameters in Graphs, Eccentricity, Radius, and Central Vertices, Adjacency Matrices and Distance Computations in Graphs and Directed Graphs, Edge and Vertex Cuts in Connected Graphs/Digraphs, Characterization of Bipartite Graphs Using Cycles, Exercises, Computer Exercises

8.3: Trees: Basic Concepts about Trees, Rooted Trees and Binary Trees, Models with Rooted Trees, Properties of Rooted Trees, Ordered Tree Traversal Algorithms, Binary Search Trees, Representing Rooted Trees on Computers, Exercises, Computer Exercises

Appendix: Application of Rooted Trees to Data Compression and Coding; Huffman Codes

Chapter 9: Graph Traversal and Optimization Problems 617

9.1: Graph Traversal Problems: Euler Paths and Tours and the Origin of Graph Theory, Euler Paths and Tours in Digraphs, Application of Eulerian Digraphs: De Bruijn Sequences, Hamilton Paths and Tours, Application of Hamiltonian Graphs: Gray Codes, Sufficient Conditions for a Graph to Be Hamiltonian, Necessary Conditions for a Graph to Be Hamiltonian, Exercises, Computer Exercises

9.2: Tree Growing and Graph Optimization Algorithms: Minimum Spanning Tree for an Edge-Weighted Graph, Tree Growing Meta-Algorithm, Prim's Algorithm for Minimum Spanning Trees, Dijkstra's Algorithm for Shortest Distances in an Edge-Weighted Connected Graph, Depth-First Searches and Breadth-First Searches, The Traveling Salesman Problem, Insertion Heuristics for the Traveling Salesman Problem, Performance Guarantees for Insertion Heuristics for the Traveling Salesman Problem, Exercises, Computer Exercises

9.3: Network Flows: Flow Networks, Cuts in Flow Networks, The Maximum Flow/Minimum Cut Theorem, The Ford-Fulkerson Maximum Flow/Minimum Algorithm, Applications of Maximum Flows, Maximum Matchings in Bipartite Graphs, Hall's Marriage Theorem, Exercises, Computer Exercises

Chapter 10: Randomized Search and Optimization Algorithms 729

10.1: Randomized Search and Optimization: An Overview: Random Search Algorithms, Hill Climbing Algorithms, The *k*-Opt Local Search Algorithm for Traveling Salesman Problems, Randomized Hill Climbing Algorithms, A Brief Discussion on Some Other Randomized Heuristic Algorithms, Tabu Search, Ant Colony Optimization, Simulated Annealing, Exercises and Computer Exercises

10.2: Genetic Algorithms: Motivating Example, The Basic Genetic Algorithm, Cloning and Inversions, Application to Ramsey Numbers, Theoretical Underpinnings, Exercises and Computer Exercises

Appendix A: Pseudo Code Dictionary 781

Appendix B: Solutions to All Exercises for the Reader 787

Appendix C: Answers/Brief Solutions to Odd Numbered Exercises 859

References 957

Index of Theorems, Propositions, Lemmas, and Corollaries 963

Index of Algorithms 967

Index 969