

A Short Course
in
Discrete Mathematics

for students of computer and computational science

Edward A. Bender
S. Gill Williamson

Preface

Discrete mathematics is an essential tool in almost all subareas of computer science. Interesting and challenging problems in discrete mathematics arise in programming languages, computer architecture, networking, distributed systems, database systems, AI, theoretical computer science, and other areas.

The course. The University of California, San Diego, has a lower-division two-quarter course sequence in discrete mathematics that includes Boolean arithmetic, combinatorics, elementary logic, induction, graph theory and finite probability. These courses are core undergraduate requirements for majors in Computer Science, Computer Engineering, and Mathematics-Computer Science. This text, *A Short Course in Discrete Mathematics*, was developed for the first quarter and *Mathematics for Algorithm and System Analysis* was developed for the second quarter.

This book consists of six units of study (Boolean Functions and Computer Arithmetic; Logic; Number Theory and Cryptography; Sets and Functions; Equivalence and Order; and Induction, Sequences and Series), each divided into two sections. Each section contains a representative selection of problems. These vary from basic to more difficult, including proofs for study by mathematics students or honors students.

The review questions. “Multiple Choice Questions for Review” appear at the end of each unit. The explanatory material in this book is directed towards giving students the mathematical language and sophistication to recognize and articulate the ideas behind these questions and to answer questions that are similar in concept and difficulty. Many variations of these questions have been successfully worked on exams by most beginning students using this book at UCSD.

Students who master the ideas and mathematical language needed to understand these review questions gain the ability to formulate, in the neutral language of mathematics, problems that arise in various applications of computer science. This skill greatly facilitates their ability to discuss problems in discrete mathematics with other computer scientists and with mathematicians.

Table of Contents

Asterisks (stars) are used in the text to mark more difficult material that is not needed in later sections.

Unit BF: Boolean Functions and Computer Arithmetic

Section 1: Boolean Functions	BF-1
Boolean function, binary operator, unary operator, not (\sim), and (\wedge), or (\vee), exclusive or (\oplus), truth table, disjunctive normal form, conjunctive normal form	
Section 2: Number Systems and Computer Arithmetic	BF-9
digit symbols, digit symbol of index or rank i , base- b number, binary arithmetic, two's complement, logic gate, half adder, full adder	
Multiple Choice Questions for Review	BF-23

Unit Lo: Logic

Section 1: Propositional Logic	Lo-1
truth table, statement forms, tautology, contradiction, implication, conditional, contrapositive, double implication, biconditional, converse, inverse, if, only if, sufficient, necessary, unless	
Section 2: Predicate Logic	Lo-12
predicate, truth set, prime, composite, Fermat number, Mersenne number, perfect numbers, Goldbach conjecture, Fermat's Last Theorem, Marin Mersenne (1588–1648), Pierre de Fermat (1601–1665), Christian Goldbach (1690–1764), Leonhard Euler (1707–1783), Karl Friedrich Gauss (1777–1855)	
Multiple Choice Questions for Review	Lo-23

Unit NT: Number Theory and Cryptography

Section 1: Basic Facts About Numbers	NT-1
rational numbers, irrational numbers, prime, composite, odd, even, n divides m , prime factorization, infinitely many primes, perfect squares, irrationality of integral square roots, residue classes mod d , mod as binary operator, mod as equivalence	

relation, modular arithmetic, modular addition, modular multiplication, floor function, ceiling function, diagonalization proofs

Section 2: Cryptography and Secrecy **NT-13**
plaintext, ciphertext, key, espionage, greatest common divisor, least common multiple, $\gcd(m, n)$ as linear combination of m and n , Euclidean algorithm, Euler ϕ function, public key, symmetric encryption, discrete log problem, Diffie-Hellman algorithm, *RSA algorithm

Multiple Choice Questions for Review **NT-26**

Unit SF: Sets and Functions

Section 1: Sets **SF-1**
intersection, union, difference, complement, symmetric difference, product, Cartesian product, binomial coefficients, $C(n, k) = \binom{n}{k}$, algebraic rules, associative rule, distributive rule, idempotent rule, DeMorgan's rule, absorption rule, commutative rule, lexicographic order, power set, characteristic function, set partitions, Bell numbers, refinement

Section 2: Functions **SF-15**
function, domain, range, codomain, image, relation, functional relation, one-line notation, surjection, onto, injection, one-to-one, bijection, permutation, two-line notation, composition of functions, cycle form of permutation, image of function, inverse image, coimage, set partitions, Stirling numbers $S(n, k)$, Bell numbers

Multiple Choice Questions for Review **SF-29**

Unit EO: Equivalence and Order

Section 1: Equivalence **EO-1**
equivalence relation, equivalence class, blocks of a partition, coimage, reflexive, symmetric, transitive, relational description, coimage description, pigeonhole principle, subset sums, monotone subsequences, extended pigeonhole principle, transpositions

Section 2: Order **EO-12**
antisymmetric relation, order relation, partially ordered set, poset, incidence matrices, total ordering, linear ordering, set inclusion, lattice of subsets, incomparable subsets, refinement relation, subposet, direct product, Cartesian product, coordinate order, characteristic function, directed graph diagrams, transitive closure, Boolean product, Boolean sum, covering relation, Hasse diagram, chain, least element, greatest element, maximal element, minimal element, lexicographic (lex) order, length-first lex order, lexicographic bucket sort, comparison sort, tiling problems, domino coverings, rotation-reflection relation, linear extensions, topological sorting

Multiple Choice Questions for Review EO-34

Unit IS: Induction, Sequences and Series

Section 1: Induction IS-1
induction, strong induction, simple induction, induction hypothesis, induction step, base case, product of primes, sum of first n integers, *sums of k^{th} powers, *differences

Section 2: Infinite Sequences IS-12
infinite sequence, limit of sequence, convergent sequence, bounded sequence, monotone sequence, convergent to infinity

***Section 3: Infinite Series** IS-20
infinite series, telescoping series, geometric series, harmonic series, alternating harmonic series, alternating series, generalized alternating series, absolute convergence, conditional convergent, tails of series, integral test, general harmonic series, convergence and intuition, the size of primes

Multiple Choice Questions for Review IS-31

Solutions to Exercises

Notation Index

Subject Index