Math 245 — Discrete Mathematics

Peter Blomgren
blomgren@mail.SDSU.EDU

Fall 2006

Basic Information

Professor	Peter Blomgren
Email	blomgren@mail.SDSU.EDU
Phone	(619)594-2602
Office	GMCS 587
Office Hours	TuTh: 3:30p-5:15p, and by appointment
Class Web Page	http://terminus.SDSU.EDU/SDSU/Math245_f2006/
Meeting Place	GMCS 307
Meeting Time	TuTh, 2:00-3:15p
Text	Susanna S. Epp, *Discrete Mathematics with Applications*, 3rd Ed.

Course Description

Discrete mathematics is an exciting and rapidly growing area of mathematics which has important applications in computer science and in many high technology areas. For example, "secure" Internet communication, efficient storage of data (e.g. jpeg, mpeg, mp3) and robust communication networks are developed using techniques from discrete mathematics.

This course serves two main populations, students from mathematics and students from computer science. The course also has two distinct goals: one is to teach the basics of set theory, logic, combinatorics and graph theory. The other is to convey concepts essential to mathematics: clarity and precision in definitions and statements of fact, and rigorous methods for establishing that a statement is true. The fundamental mathematics taught in this course is critical to understanding computer languages and to the development of good programming skills.

Student Evaluation

We will have weekly assignments (due in GMCS 587 by noon on Fridays), two (2) midterms and a final exam. For the weekly assignments there will be a small number of problems (10 or so) which you should write up carefully. They will be graded and returned to you.

Start the assignments early and do most of the exercises in each section we cover. If you get stuck, please ask me in class and/or office hours. Your questions often lead to a valuable class discussion.

Covered Topics

The Logic of Compound Statements

§1.1 — Logical Form and Logical Equivalence

Statements; Compound statements; Truth values; Evaluating the truth of more general compound statements; Logical equivalence; Tautologies and contradictions.

§1.2 — Conditional Statements

Logical equivalence involving "→"; Representation of *if-then* as *or*; The negation of a conditional statement; The contrapositive of a conditional statement; *Only if* and the bi-conditional; Necessary and sufficient conditions.

§1.3 — Valid and Invalid Arguments

Modus ponens and *modus tollens*; Additional valid argument forms; Rules of inference; Fallacies; Contradiction and valid arguments.

§1.4 — Application: Digital Logic Circuits

Black boxes and gates; The input/output for a circuit; The boolean expression corresponding to a circuit; The circuit corresponding to a boolean expression; Finding a circuit that corresponds to a given input/output table; Simplifying combinatorial circuits; NAND and NOR gates.

The Logic of Quantified Statements

§2.1 — Introduction to Predicates and Quantified Statements I

The universal quantifier "$\forall$"; The existential quantifier "$\exists$"; Formal versus informal language; Universal conditional statements; Equivalence forms of universal and existential statements; Implicit quantification; Tarski's World.

§2.2 — Introduction to Predicates and Quantified Statements II

Negations of quantified statements; Negations of universal conditional statements; The relation among $\forall$, $\exists$, $\wedge$, $\vee$; Vacuous truth of universal statements; Variants of universal conditional statements; Necessary and sufficient conditions, *only if*.

§2.3 — Statements Containing Multiple Quantifiers

Translating from informal to formal language; Ambiguous language; Negations of multiply-quantified statements; Order of quantifiers; Formal logical notation.

§2.4 — Arguments with Quantified Statements

Universal *modus ponens*; Use of universal *modus ponens* in a proof; Universal *modus tollens*; Proving validity of arguments with quantified statements; Using diagrams to test for validity; Creating additional forms of argument; Converse and inverse error.

Elementary Number Theory and Methods of Proof

§3.1 — Direct Proof and Counterexample I: Introduction

Definitions; Proving existential statements; disproving universal statements by counterexample; Proving universal statements; Directions for writing proofs of universal statements; Common mistakes; Getting proofs started; Showing that an existential statement is false; Conjecture, proof, and disproof.

§3.2 — Direct Proof and Counterexample II: Rational Numbers

More on generalizing from the generic particular; Proving properties of rational numbers; Deriving new mathematics from old.

§3.3 — Direct Proof and Counterexample III: Divisibility

Definition of divisibility; Examples and properties; The unique factorization theorem.

§3.4 — Direct Proof and Counterexample IV: Division into Cases and the Quotient-Remainder Theorem

Discussion of the quotient-remainder theorem and examples; *div* and *mod*; Alternate representations of integers and applications to number theory.

§3.5 — Direct Proof and Counterexample V: Floor and Ceiling

Definition and basic properties; The floor of $n/2$.

§3.6 — Indirect Argument: Contradiction and Contraposition

Proof by contradiction; Argument by contraposition; Relation between proof by contradiction and proof by contraposition; Proof as a problem-solving tool.

§3.7 — Two Classical Theorems

The irrationality of $\sqrt{2}$; The infinitude of the set of prime numbers; When to use indirect proof; Open questions in number theory.

Sequences and Mathematical Induction

§4.1 — Sequences

Explicit formulas for sequences; Summation notation; Product notation; Factorial notation; Properties of summations and products; Change of variable; Sequences in computer programming; Application: algorithm to convert from base 10 (decimal) to base 2 (binary) using repeated division by 2.

§4.2 — Mathematical Induction I

Principle of mathematical induction; Sum of the first n integers; Sum of a geometric sequence.

§4.3 — Mathematical Induction II

Comparison of mathematical induction and inductive reasoning; Proving divisibility properties; Proving inequalities.

§4.4 — Strong Mathematical Induction and the Well-Ordering Principle

Principle of strong mathematical induction; binary representation of integers; The well-ordering principle for the integers.

Set Theory

§5.1 — Basic Definition of Set Theory

Subsets; Set equality; Operations on sets; Venn diagrams; The empty set; Partitions of sets; Power sets; Cartesian products; Algorithm for checking a subset relation.

§5.2 — Properties of Sets

Set identities; Proving set identities; Proving that a set is the empty set.

§5.3 — Disproofs, Algebraic Proofs, and Boolean Algebras

Disproving an alleged set property; Problem-solving strategy; The number of subsets of a set; "Algebraic" proofs of set identities; Boolean algebras.

Counting

§6.1 — Counting and Probability

Definition of sample space and even; Probability in the equally likely case; Counting the elements of lists, sublists, and one-dimensional arrays.

§6.2 — Possibility Trees and the Multiplication Rule

Possibility trees; The multiplication rule; When the multiplication rule is difficult or impossible to apply; Permutations; Permutations of selected elements.

§6.3 — Counting Elements of Disjoint Sets: The Addition Rule

The addition rule; The difference rule; The inclusion/exclusion rules.

§6.4 — Counting Subsets of a Set: Combinations

r-combinations; Ordered and unordered selections; Relation between permutations and combinations; Permutations of a set with repeated elements; Some advice about counting.

§6.5 — r-Combinations with Repetition Allowed

Multi-sets and How to count them; Which formula to use?

§6.6 — The Algebra of Combinations

Combinatorial formulas; Pascal's triangle; Algebraic and combinatorial proofs of Pascal's formula.

§6.7 — The Binomial Theorem

The binomial theorem; Algebraic and combinatorial proofs.

§6.8 — Probability Axioms and Expected Value

Probability axioms; Deriving additional probability formulas; Expected value.

§6.9 — Conditional Probability, Bayes' Formula, and Independent Events

Conditional probability; Bayes' theorem; Independent events.

Functions

§7.1 — Functions Defined on General Sets

Definition of a function; Arrow diagrams; Function machines; Examples of functions; Boolean functions; Checking whether a function is well-defined.

§7.2 — One-to-One and Onto, Inverse Functions

One-to-one functions; One-to-one functions on infinite sets; Application: hash functions; Onto functions; Onto functions on infinite sets; Properties of logarithmic and exponential functions; One-to-one correspondences; Inverse functions.

§7.3 — Application: The Pigeonhole Principle

Statement and discussion of the principle; Applications; Decimal expansion of fractions; Generalized pigeonhole principle; Proof of the pigeonhole principle.

§7.4 — Composition of Functions

Definition and examples; Composition of one-to-one functions; Composition of onto functions.

Recursion

§8.1 — Recursively Defined Sequences

Definition of recurrence relation; Examples of recursively defined sequences; Number of partitions of a set into r subsets.

§8.2 — Solving Recurrence Relations by Iteration

The method of iteration; Using formulas to simplify solutions obtained by iteration; Checking the correctness of a formula by mathematical induction; Discovering that an explicit formula is incorrect.

§8.3 — Second-Order Linear Homogeneous Recurrence Relations with Constant Coefficients

Derivation of technique for solving these relations; The distinct-root case; The single-root case.

Relations

§10.1 — Relations on Sets

Definition of Binary Relation; Arrow diagram of a relation; Relations and functions; The inverse of a relation; Directed graph of a relation; n-ary relations and relational databases.

§10.2 — Reflexivity, Symmetry, and Transitivity

Reflexive, symmetric, and transitive properties; The transitive closure of a relation; Properties of relations on infinite sets.

§10.3 — Equivalence Relations

The relation induced by a partition; Definition of equivalence relation; Equivalence classes of an equivalence relation.

§10.4 — Modular Arithmetic with Applications to Cryptography

Properties of congruence modulo n; Modular arithmetic; Finding an inverse modulo n; Euclid's lemma; Fermat's little theorem and the Chinese remainder theorem; Why does the RSA cipher work?

§10.5 — Partial Order Relations

Antisymmetry; Partial order relations; Lexicographic order; Hasse diagrams; Partially and totally ordered sets; Topological sorting.

Revision information: `$Id: syllabus.tex,v 1.5 2006/08/28 20:56:51 blomgren Exp $`