INFORMATION & COMPUTER SCIENCES
UNIVERSITY of HAWAI'I at MĀNOA

Course Review

ICS 141: Discrete Mathematics for Computer Science I

KYLE BERNEY
DEPARTMENT OF ICS, UNIVERSITY OF HAWAII AT MANOA

Logic

- Propositions
  - Operators
    - Negation ($\neg$)
    - Conjunction ($\wedge$)
    - Disjunction ($\vee$)
    - Exclusive Or ($\oplus$)
    - Conditional Statement ($\Rightarrow$)
    - Biconditional Statement ($\Leftrightarrow$)
  - Truth Tables

Logic

- Propositions
  - Logical Equivalences
    - Tautology
    - Contradiction
    - Contingency

Logic

- Propositions
  - Logical Equivalences
    - De Morgan's Laws
    - Conditional Disjunction
    - Distributive Laws
    - Identity Laws
    - Domination Laws
    - Idempotent Laws
    - Negation Laws
    - Commutative Laws
    - Associative Laws
    - Absorption Laws
    - Conditional and Biconditional Equivalences

Logic

- Predicates and Quantifiers
  - Operators
    - Universal Quantifier ($\forall$)
    - Existential Quantifier ($\exists$)
    - Uniqueness Quantifier ($\exists!$)
  - De Morgan's Laws

Proofs

- Proof Methods
  - Direct Proof
  - Proof by Contraposition
  - Proof by Contradiction
  - Proof by Induction
  - Vacuous Proof
  - Trivial Proof
  - Proof by Cases

Sets

- Set membership ($\in$)
- Empty set ($\emptyset$)
- Defining a set
  - Demonstrate a pattern (using . . . to extrapolate the pattern)
  - Set builder notation
- Subsets and supersets
  - Proper subset/superset ($\subset$)
  - Subset/superset ($\subseteq$)
- Power Sets ($\mathcal{P}$)
- Disjoint Sets

Sets

- Notable Sets
  - Natural numbers, $\mathbb{N}$
  - Integers, $\mathbb{Z}$
    - Positive integers, $\mathbb{Z}^+$
    - Negative integers, $\mathbb{Z}^-$
  - Rational numbers, $\mathbb{Q}$
  - Real numbers, $\mathbb{R}$
    - Positive real numbers, $\mathbb{R}^+$
    - Negative real numbers, $\mathbb{R}^-$
  - Complex numbers, $\mathbb{C}$

Sets

- Operators
  - Cartesian Product ($\times$)
  - Union ($\cup$)
  - Intersection ($\cap$)
  - Set difference ($-$)
  - Complement ($\overline{A}$)

Sets

- Set identities
  - De Morgan's Laws
  - Distributive Laws
  - Identity Laws
  - Domination Laws
  - Idempotent Laws
  - Complementation Laws
  - Complement Laws
  - Commutative Laws
  - Associative Laws
  - Absorption Laws

Sets

- Set equality
  1. Subset method
  2. Membership table
  3. Apply set identities
- Cardinality
  - Countable
  - Uncountable

Functions

- Let $f : A \to B$, such that $f(a) = b$
- Terminology:
  - A is the domain
  - B is the codomain
  - b is the image of a
  - a is the preimage of b
  - Range of f is the set of all images of $a \in A$

Functions

- Injective (one-to-one)
- Surjective (onto)
- Bijection (one-to-one mapping)
- Notable functions:
  - Identity function, ι
  - Inverse function, f^{-1}
  - Floor function, $\lfloor n \rfloor$
  - Ceiling function, $\lceil n \rceil$
  - Factorial, $n!$
  - Exponential, b^n
  - Logarithm, $\log_b a$

Sequences

- Finite sequences
- Infinite sequences
- Notable sequences:
  - Geometric progression
  - Arithmetic progression
  - Strings
  - Fibonacci sequence
- Recurrence relations

Summations

- Notable summations:
  - Arithmetic series
  - Sum of squares
  - Sum of cubes
  - Geometric series
  - Harmonic series
  - Telescoping series
- Product of terms in a sequence
  - Telescoping series

Matrices

- Matrix Operations
  - Addition / Subtraction
  - Multiplication
  - Powers of square matrices
  - Transpose
- Identity matrix

Algorithms

- Pseudocode
- Searching algorithms
  - Linear search
  - Binary search
- Sorting algorithms
  - Bubble sort
  - Insertion sort
  - Merge sort
- String matching
- Optimization problems
  - Greedy algorithms

Algorithms

- Asymptotic analysis
  - Big O, O
  - Big Omega, Ω
  - Theta, Θ
  - Little o, o
  - Little omega, ω
- Analyzing iterative algorithms via summations
- Proof of correctness
  - Loop invariants
  - Proof by induction

Number Theory

- Divisibility
  - Division algorithm
- Modular Arithmetic
  - Residue classes
  - Reduced residue
- Representation of integers
  - Decimal (base 10)
  - Binary (base 2)
  - Octal (base 8)
  - Hexadecimal (base 16)

Number Theory

- Greatest common divisor (GCD)
  - Euclidean algorithm
  - Extended Euclidean algorithm
- Least common multiple (LCM)
- Primes and Composite integers
  - Linear combinations
  - Fundamental Theorem of Arithmetic
  - Trial division
    - Primality testing
    - Prime factorization

Number Theory

- Linear congruences
- Inverse modulo m
- Systems of linear congruences
  - Chinese Remainder Theorem
- Cryptography (*Not covered on final exam*)
  - Caesar cipher
  - Affine cipher
  - Transposition cipher
  - RSA cryptosystem

Counting

- Product rule
- Sum rule
- Subtraction rule
  - Inclusion-exclusion principle
- Division rule
- Pigeonhole principle
- Permutations
- Combinations
- Binomial Coefficients
  - Binomial Theorem
  - Pascal's Triangle

Probability

- Finite probability
- Probability distribution
  - Uniform distribution
- Conditional probability
  - Bayes' Theorem
- Independence
  - Pairwise independence
  - Mutual independence
- Bernoulli trials

Probability

- Random Variables
  - Indicator random variables
  - Expected value
  - Linearity of expectations
  - Variance