Final Exam Review

CMPS/MATH 2170: Discrete Mathematics

Overview

- Final Exam
  - Format: similar to midterm, closed book, one page cheat sheet allowed
  - Time & Place: **Monday, Dec 10, 10 AM – 12 PM,** Stanley Thomas 302
- Office hours on Sunday Dec 9: 12-2pm
- Course evaluations (end on Dec 9)
  - Gibson → "course evaluations"

Topics (before midterm, 30%)

- Logic: 1.1-1.6
- Proofs: 1.7-1.8
- Sets and Functions : 2.1-2.3, 2.5
- Mathematical Induction: 5.1

Topics (after midterm, 70%)

- Sequences: 2.4
- Strong Induction: 5.2
- Recursion: 5.3, ~~8.1~~
- Number Theory: 4.1, 4.3, 4.4, ~~4.6~~
- Counting: 6.1-6.3, 6.5
- Discrete Probability: 7.1, 7.2, 7.4

Sequences (2.4)

- Know how to define a sequence
  - List all the elements
  - Define a sequence as a function
  - Recursive definition
- Arithmetic and geometric progressions and their summations
- Fibonacci Sequence
  - Using strong induction to prove properties of Fibonacci sequence

Strong Induction (5.2)

- Know how to prove $\forall n \in \mathbb{Z}^+ \colon P(n)$ using strong induction

  Proof by strong induction on n:

  - Base case: verify that $P(1)$ is true, $P(2)$ is true, …
  - Inductive step: show that $[P(1) \wedge P(2) \wedge \ \ldots \wedge P(k)] \rightarrow P(k+1)$ for any $k \in \mathbb{Z}^+$

- The base case is not necessarily $n = 1$, and there may have multiple base cases

Recursive Definitions (5.3)

- Know how to define a discrete structure (e.g., sequence, function, or set) recursively
  - Initial conditions
  - Recurrence relation
- Play with a recursive definition
  - E.g., if $f(n) = f\left(\frac{n}{3}\right) + 2n$ and $f(1) = 1$. Find $f(27)$.

Division and Primes (4.1,4.3)

- Division
  - $a \mid b \Leftrightarrow b = ka$ for some $k \in \mathbb{Z}$
- Primes
  - the Fundamental theorem of Arithmetic
  - A composite n has a prime divisor $\leq \sqrt{n}$
  - there are infinite many primes
- Great common divisor and least common multiple

Division Algorithms (4.3)

- Division algorithm: $a = dq + r,\ 0 \le r < d$
  - $q = a \operatorname{div} d, r = a \bmod d$
  - $\gcd(a, d) = \gcd(d, r)$
- Euclidean algorithm
  - find gcd by successively applying the division algorithm
- Bezout's Theorem: $\gcd(a, b) = sa + tb$
  - If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$

Congruences (4.1,4.4)

- Congruences
  - $a \equiv b \pmod{m} \Leftrightarrow \ m \mid (a - b) \ \Leftrightarrow \ (a \bmod m) = (b \bmod m)$
- $\mathbb{Z}_m$ and Arithmetic Modulo m
- Multiplicative inverse: $a \cdot b \equiv 1 \pmod{m}$
  - a has a multiplicative inverse modulo m if and only if $\gcd(a, m) = 1$.
  - $\gcd(a, m) = 1 \Rightarrow \ sa + tm \equiv 1 \pmod{m} \ \Rightarrow sa \equiv 1 \pmod{m}$
- Solving Linear Congruences: $ax \equiv b \pmod{m}$
- Fermat's Little Theorem
  - compute $a^n \bmod p$ where p is prime and $p \nmid a$
- ~~Fast Modular Exponentiation~~

Counting (6.1-6.2)

- The product rule, the sum rule, the subtraction rule (6.1)
  - Break the problem into stages ⇒ product rule
  - Break the problem into disjoint subcases ⇒ sum rule
    - If the subcases are non-disjoint ⇒ subtraction rule
  - For more complicated problems, product and sum rules are often used together
- The Pigeonhole Principle (6.2)
  - Generalized Pigeonhole Principle

Permutations and Combinations (6.3, 6.5)

	Permutations	Combinations
Without repetition (6.3)	$P(n,r) = \frac{n!}{(n-r)!}$	$C(n,r) = \binom{n}{r} = \frac{n!}{r!\,(n-r)!}$
With repetition (6.5)	n^r	$\binom{n+r-1}{r}$

How many bit strings of length 8?

How many bit strings of length 8 have exactly three 1's?

Discrete Probability (7.1-7.2)

- Discrete probability laws
  - For a given experiment, identify the set of outcomes and their probabilities
  - know how to compute the probability of an event $\mathrm{P}(A) = \sum_{s \in A} \mathrm{P}(\{s\})$
- Basic properties
  - $\mathrm{P}(\overline{A}) = 1 - \mathrm{P}(A)$, $\mathrm{P}(A \cup B) = \mathrm{P}(A) + \mathrm{P}(B) - \mathrm{P}(A \cap B)$

Independence (7.2)

- Independence: $\mathrm{P}(A \cap B) = \mathrm{P}(A)\,\mathrm{P}(B)$
  - Know how to determine if two given events are independent or not
- Independent Bernoulli Trials
  - p - probability of heads
  - The probability of having exactly k heads is $\binom{n}{k} p^k (1-p)^{n-k}$

Random Variables (7.2, 7.4)

- Random variables: real-valued functions of the experiment outcome
  - Know how to compute probabilities for events defined by random variables
- Expected values: $E(X) = \sum_{s \in \Omega} X(s) \, \mathrm{P}(\{s\})$
  - Know how to find the expected value of a discrete random variable
  - The expected number of heads in independent Bernoulli trials

- A coin is flipped 6 times where each flip comes up heads or tails. How many possible outcomes contain the same number of heads as tails?

- We randomly select a permutation of the set $\{A, B, C, D\}$. What is the probability that A immediately precedes D in this permutation?

- Considering rolling a fair six-sided die. Let $A = \{\text{roll is at least } 3\}$ and $B = \{\text{roll is an odd number}\}$.
  - a. Find the probability $P(A)$
  - b. Find the probability $P(B)$
  - c. Are A and B independent?

- Consider a quiz game where a person is given two questions. Question 1 will be answered correctly with probability 0.8, and the person will then receive a prize of $100, while Question 2 will be answered correctly with probability 0.5, and the person will then receive a prize of $200. The person is allowed to answer Question 2 only if Question 1 is answered correctly. What is the expected value of the total prize money received?