Week 7 - Wednesday

COMP 2230

Last time

- More on relations
- Properties
  - Reflexive
  - Symmetric
  - Transitive
- Started equivalence classes

Questions?

Assignment 3

Back to Equivalence Relations

Partitions

- A partition of a set A (as we discussed earlier) is a collection of nonempty, mutually disjoint sets, whose union is A
- A relation can be induced by a partition
- For example, let $A = \{0, 1, 2, 3, 4\}$
- Let A be partitioned into $\{0, 3, 4\}, \{1\}, \{2\}$
- The binary relation induced by the partition is: $x\ R\ y \leftrightarrow x$ and y are in the same subset of the partition
- List the ordered pairs in R

Equivalence relations

- Given set A with a partition
- Let R be the relation induced by the partition
- Then, R is reflexive, symmetric, and transitive
- As it turns out, **any** relation R is that is reflexive, symmetric, and transitive induces a partition
- We call a relation with these three properties an **equivalence relation**

Congruences

- We say that m is congruent to n modulo d if and only if $d \mid (m - n)$
- We write this:
  - $m \equiv n \pmod{d}$
- Congruence mod d defines an equivalence relation
  - Reflexive, because $m \equiv m \pmod{d}$
  - Symmetric because $m \equiv n \pmod{d}$ means that $n \equiv m \pmod{d}$
  - Transitive because $m \equiv n \pmod{d}$ and $n \equiv k \pmod{d}$ mean that $m \equiv k \pmod{d}$
- Which of the following are true?
  - $12 \equiv 7 \pmod{5}$
  - $6 \equiv -8 \pmod{4}$
  - $3 \equiv 3 \pmod{7}$

Equivalence classes

- Let A be a set and R be an equivalence relation on A
- For each element a in A, the **equivalence class of** a, written $[a]$, is the set of all elements x in A such that $a\ R\ x$
- Example
  - Let A be $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$
  - Let R be congruence $\mathrm{mod}\ 3$
  - What's the equivalence class of 1?
- For A with R as an equivalence relation on A
  - If $b \in [a]$, then $[a] = [b]$
  - If $b \notin [a]$, then $[a] \cap [b] = \emptyset$

Equivalence relation practice

- Let $A = \mathbb{R} \times \mathbb{R}$. A relation F is defined on A as follows:
  - For all (x_1, y_1) and (x_2, y_2) in A, $(x_1, y_1)\ F\ (x_2, y_2) \leftrightarrow x_1 = x_2$.
  - Is F equivalence relation?
- Let A be the set of people living in the world today. A relation R is defined on A as follows:
  - For all $p, q \in A$, $p\ R\ q \leftrightarrow p$ lives within 100 miles of q.
  - Is R an equivalence relation?

Modular Arithmetic

Modular arithmetic

- Modular arithmetic has many applications
  - Many of them in cryptography
- To help us, the following statements for integers a, b, and n, with $n > 1$, are all equivalent:
  1. $n \mid (a - b)$
  2. $a \equiv b \pmod{n}$
  3. $a = b + kn$ for some integer k
  4. a and b have the same remainder when divided by n
  5. $a \bmod n = b \bmod n$

Rules of modular arithmetic

- Let a, b, c, d and n be integers with $n > 1$
- Let $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then:
  1. $(a + b) \equiv (c + d) \pmod{n}$
  2. $(a - b) \equiv (c - d) \pmod{n}$
  3. $ab \equiv cd \pmod{n}$
  4. $a^m \equiv c^m \pmod{n}$, for all positive integers m
- If a and n are relatively prime (share no common factors), then there is a multiplicative inverse a^{-1} such that $a^{-1} \cdot a \equiv 1 \pmod{n}$
- I'd love to have us learn how to find this, but there isn't time

Partial Orders

Antisymmetry

- Let R be a relation on a set A
- R is **antisymmetric** iff for all a and b in A, if $a \; R \; b$ and $b \; R \; a$, then $a = b$
- That is, if two different elements are related to each other, then the relation is **not** antisymmetric
- Let R be the "divides" relation on the set of all positive integers
- Is R antisymmetric?
- Let S be the "divides" relation on the set of all integers
- Is S antisymmetric?

Partial orders

- A relation that is reflexive, antisymmetric, and transitive is called a **partial order**
- The subset relation is a partial order
  - Show it's reflexive
  - Show it's antisymmetric
  - Show it's transitive
- The less than or equal to relation is a partial order
  - Show it's reflexive
  - Show it's antisymmetric
  - Show it's transitive

Hasse Diagrams

- Let set $A = \{1, 2, 3, 9, 18\}$
- Let R be the "divides" relation on A
- Draw A as a set of points and connect each pair of points with arrows if they are related with R
- Now, delete all loops and transitive arrows
- This is a **Hasse Diagram**

Total orders

- Let R be a partial order on set A
- Elements $a, b \in R$ are **comparable** if either $a\ R\ b$ or $b\ R\ a$ (or both)
- If all the elements in a partial order are comparable, then the partial order is a total order
- Let R be the "less than or equal to" relation on $\mathbb{R}$
  - Is it a total order?
- Let S be the "divides" relation on positive integers
  - Is it a total order?

Review

Indirect Proofs

Proof by contradiction

- In a proof by contradiction, you begin by assuming the negation of the conclusion
- Then, you show that doing so leads to a logical impossibility
- Thus, the assumption must be false and the conclusion true

Contradiction formatting

- A proof by contradiction is different from a direct proof because you are **trying** to get to a point where things don't make sense
- You should always mark such proofs clearly
- Start your proof with the words **Proof by contradiction**
- Write **Negation of conclusion** as the justification for the negated conclusion
- Clearly mark the line when you have both p and $\sim p$ as a **contradiction**
- Finally, state the conclusion with its justification as the contradiction found before

Sequences and Induction

Sequences

- Mathematical sequences can be represented in **expanded form** or with **explicit formulas**
- Examples:
  - $2, 5, 10, 17, 26, \ldots$
  - $a_i = i^2 + 1, \quad i \geq 1$
- **Summation notation** is used to describe a summation of some part of a sequence

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + a_{m+2} + \ldots + a_n$$

- **Product notation** is used to describe a product of some part of a sequence

$$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot a_{m+2} \cdot \ldots \cdot a_n$$

Proof by mathematical induction

- To prove a statement of the following form:
  - $\forall n \in \mathbb{Z}$, where $n \geq a$, property $P(n)$ is true
- Use the following steps:

1. Basis Step: Show that the property is true for $P(a)$
2. Induction Step:
   - Suppose that the property is true for some $n = k$, where $k \in \mathbb{Z}, k \geq a$
   - Now, show that, with that assumption, the property is also true for $k + 1$

Mathematical induction example

- Prove that, for all integers $n \geq 1$,

$$\frac{\sum_{i=1}^{n} 2i - 1}{\sum_{i=1}^{n} 2n + 2i - 1} = \frac{1}{3}$$

Recursion

- Using recursive definitions to generate sequences
- Writing a recursive definition based on a sequence
- Using mathematical induction to show that a recursive definition and an explicit definition are equivalent

Employing outside formulas

- Sure, intelligent pattern matching gets you a long way
- However, it is sometimes necessary to substitute in some known formula to simplify a series of terms
- Recall
  - Geometric series: $1 + r + r^2 + \cdots + r^n = \frac{r^{n+1}-1}{r-1}$
  - Arithmetic series: $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$

Recursive sequence example

- $g_k = \frac{g_{k-1}}{g_{k-1}+2}$ for all integers $k \geq 1$
- g_0 = 1

- Give an explicit formula for this recurrence relation
- **Hint:** Use the method of iteration

Solving second order linear homogeneous recurrence relations with constant coefficients

- To solve sequence $a_k = Aa_{k-1} + Ba_{k-2}$
- Find its characteristic equation $t^2 - At - B = 0$
- If the equation has two distinct roots r and s
  - Substitute a_0 and a_1 into $a_n = Cr^n + Ds^n$ to find C and D
- If the equation has a single root r
  - Substitute a_0 and a_1 into $a_n = Cr^n + Dnr^n$ to find C and D
- **There will be one of these on the exam**

Set Theory

Set theory basics

- Defining finite and infinite sets
- Definitions of:
  - Subset
  - Proper subset
  - Set equality
- Set operations:
  - Union
  - Intersection
  - Difference
  - Complement
- The empty set
- Partitions
- Cartesian product

Set theory proofs

- Proving a subset relation
  - Element method: Assume an element is in one set and show that it must be in the other set
  - Algebraic laws of set theory: Using the algebraic laws of set theory (given on the next slide), we can show that two sets are equal
- Disproving a universal statement requires a counterexample with specific sets

Laws of set theory

Name	Law	Dual
Commutative	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associative	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$
Distributive	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Identity	$A \cup \emptyset = A$	$A \cap U = A$
Complement	$A \cup A^c = U$	$A \cap A^c = \emptyset$
Double Complement	$(A^c)^c = A$	
Idempotent	$A \cup A = A$	$A \cap A = A$
Universal Bound	$A \cup U = U$	$A \cap \emptyset = \emptyset$
De Morgan's	$(A \cup B)^c = A^c \cap B^c$	$(A \cap B)^c = A^c \cup B^c$
Absorption	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Complements of U and $\emptyset$	$U^c = \emptyset$	$\emptyset^c = U$
Set Difference	$A - B = A \cap B^c$	

Set theory proof example

- Use the element method to prove the following:
- For all sets A, B, and C, if $A \subseteq B$ then $A \cap C \subseteq B \cap C$

Russell's paradox

- It is possible to give a description for a set which describes a set that does not actually exist
- For a well-defined set, we should be able to say whether or not a given element is or is not a member
- If we can find an element that must be in a specific set and must not be in a specific set, that set is not well defined
- **Watch out for definitions that are logically inconsistent!**

Functions

- **One-to-one** (**injective**) functions
- **Onto** (**surjective**) functions
- If a function is both one-to-one and onto, we call it **bijective**

Cardinality

- Cardinality is the number of things in a set
  - It is reflexive, symmetric, and transitive
- Two sets have the same cardinality if a bijective function maps every element in one to an element in the other
- Any set with the same cardinality as positive integers is called **countably infinite**

Relations

- **Relations** are generalizations of functions
- In a function, an element of the domain must map to exactly one element of the co-domain
- In a relation, an element from one set can be related to any number (from zero up to infinity) of other elements
- Like functions, we're usually going to focus on binary relations
- We can define any binary relation between sets A and B as a subset of $A \times B$

Properties

- Relation R is **reflexive** iff for all $x \in A$, $(x, x) \in R$
  - R is **not** reflexive if there is an $x \in A$, such that $(x, x) \notin R$
- Relation R is **symmetric** iff for all $x, y \in A$, if $(x, y) \in R$ then $(y, x) \in R$
  - R is **not** symmetric if there is an $x, y \in A$, such that $(x, y) \in R$ but $(y, x) \notin R$
- Relation R is **transitive** iff for all $x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$
  - R is **not** transitive if there is an $x, y, z \in A$, such that $(x, y) \in R$ and $(y, z) \in R$ but $(x, z) \notin R$
- Relation R is **antisymmetric** iff for all a and b in A, if $a\ R\ b$ and $b\ R\ a$, then $a = b$
  - If two different elements are related to each other, then the relation is **not** antisymmetric

Kinds of relations

- Any relation R is that is reflexive, symmetric, and transitive induces a partition
  - We call a relation with these three properties an **equivalence relation**
- Any relation R that is reflexive, antisymmetric, and transitive is called a **partial order**

Upcoming

Next time…

- Exam 2!

Reminders

- Work on Assignment 3
  - Due Friday
- No office hours on Wednesday, Thursday, or Friday
- No class on Friday
- Study for Exam 2
  - Next Monday!