

Week 8 - Friday

COMP 2230

Last time

- Properties of relations:
 - Reflexive
 - Symmetric
 - Transitive
- Equivalence relations

Questions?

Assignment 4

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 and Partial Orders

Three-sentence summary

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 $a, b \in A$ 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?

Propositional Logic Review

Propositional logic

- Statements
- AND, OR, NOT, IMPLIES
- Truth tables
- Logical equivalence
- De Morgan's laws
- Tautologies and contradictions

Laws of Boolean algebra

Name	Law	Dual
Commutative	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Associative	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Identity	$p \wedge t \equiv p$	$p \vee c \equiv p$
Negation	$p \vee \sim p \equiv t$	$p \wedge \sim p \equiv c$
Double Negative	$\sim(\sim p) \equiv p$	
Idempotent	$p \wedge p \equiv p$	$p \vee p \equiv p$
Universal Bound	$p \vee t \equiv t$	$p \wedge c \equiv c$
De Morgan's	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
Absorption	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Negations of t and c	$\sim t \equiv c$	$\sim c \equiv t$

Implications

- Can be used to write an if-then statement
- Contrapositive is logically equivalent
- Inverse and converse are not (though they are logically equivalent to each other)
- Biconditional:
 - $p \rightarrow q \wedge q \rightarrow p$

Predicate Logic Review

Predicates

- A **predicate** is a sentence with a fixed number of variables that becomes a **statement** when specific values are substituted for to the variables
- The **domain** gives all the possible values that can be substituted
- The **truth set** of a predicate $P(x)$ are those elements of the domain that make $P(x)$ true when they are substituted

Sets

- We will frequently be referring to various sets of numbers in this class
- Some typical notation used for these sets:

Symbol	Set	Examples
$\mathbb{R}$	Real numbers	Virtually everything
$\mathbb{Z}$	Integers	$\{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{Z}^-$	Negative integers	$\{-1, -2, -3, \dots\}$
$\mathbb{Z}^+$	Positive integers	$\{1, 2, 3, \dots\}$
$\mathbb{N}$	Natural numbers	$\{1, 2, 3, \dots\}$
$\mathbb{Q}$	Rational numbers	a/b where $a, b \in \mathbb{Z}$ and $b \neq 0$

- Some authors use $\mathbb{Z}^+$ to refer to non-negative integers and only $\mathbb{N}$ for the natural numbers

Quantifiers

- The universal quantifier $\forall$ means "for all"
- The statement "All DJ's are mad ill" can be written more formally as:
 - $\forall x \in D, M(x)$
 - Where D is the set of DJ's and $M(x)$ denotes that x is mad ill
- The existential quantifier $\exists$ means "there exists"
- The statement "Some emcee can bust a rhyme" can be written more formally as:
 - $\exists y \in E, B(y)$
 - Where E is the set of emcees and $B(y)$ denotes that y can bust a rhyme

Negating quantified statements

- When doing a negation, negate the predicate and change the universal quantifier to existential or vice versa
- Formally:
 - $\sim(\forall x, P(x)) \equiv \exists x, \sim P(x)$
 - $\sim(\exists x, P(x)) \equiv \forall x, \sim P(x)$
- Thus, the negation of "Every dragon breathes fire" is "There is one dragon that does not breathe fire"

Vacuously true

- Any statement with a universal quantifier whose domain is the empty set is **vacuously true**
- When we talk about "all things" and there's nothing there, we can say anything we want
- "All mythological creatures are real."
- Every single one of the (of which there are none) is real

Conditionals

- Recall:
 - Statement: $p \rightarrow q$
 - Contrapositive: $\sim q \rightarrow \sim p$
 - Converse: $q \rightarrow p$
 - Inverse: $\sim p \rightarrow \sim q$
- These can be extended to universal statements:
 - Statement: $\forall x, P(x) \rightarrow Q(x)$
 - Contrapositive: $\forall x, \sim Q(x) \rightarrow \sim P(x)$
 - Converse: $\forall x, Q(x) \rightarrow P(x)$
 - Inverse: $\forall x, \sim P(x) \rightarrow \sim Q(x)$
- Similar properties relating a statement equating a statement to its contrapositive (but not to its converse and inverse) apply

Multiple quantifiers

- With multiple quantifiers, we imagine that corresponding "actions" happen in the same order as the quantifiers
- The action for $\forall x \in A$ is something like, "pick any x from A you want"
- Since a "for all" must work on everything, it doesn't matter which you pick
- The action for $\exists y \in B$ is something like, "find some y from B "
- Since a "there exists" only needs one to work, you should try to find the one that matches

Negating or changing multiple quantifiers

- For negation,
 - Simply switch every $\forall$ to $\exists$ and every $\exists$ to $\forall$
 - Then negate the predicate
- Changing the order of quantifiers can change the truth of the whole statement but does not always
- Furthermore, quantifiers of the same type are commutative:
 - You can reorder a sequence of $\forall$ quantifiers however you want
 - The same goes for $\exists$
 - Once they start overlapping, however, you can't be sure anymore

Proofs Review

Proving existential statements and disproving universal ones

- To prove $\exists x \in D, P(x)$ we need to find at least one element of D that makes $P(x)$ true
- To disprove $\forall x \in D, P(x) \rightarrow Q(x)$, we need to find an x that makes $P(x)$ true and $Q(x)$ false

Proving universal statements

- If the domain is finite, we can use the **method of exhaustion**, by simply trying every element
- Otherwise, we can use a **direct proof**
 1. Express the statement to be proved in the form $\forall x \in D$, if $P(x)$ then $Q(x)$
 2. Suppose that x is some specific (but arbitrarily chosen) element of D for which $P(x)$ is true
 3. Show that the conclusion $Q(x)$ is true by using definitions, other theorems, and the rules for logical inference
- Direct proofs should start with the word **Proof**, end with a box or the text **QED**, and have a justification for every step in the argument
- For proofs with cases, number each case clearly and show that you have proved the conclusion for all possible cases

Definitions

- If n is an integer, then:
 - n is even $\leftrightarrow \exists k \in \mathbb{Z}, n = 2k$
 - n is odd $\leftrightarrow \exists k \in \mathbb{Z}, n = 2k + 1$
- If n is an integer where $n > 1$, then:
 - n is prime $\leftrightarrow \forall r \in \mathbb{Z}^+, \forall s \in \mathbb{Z}^+, \text{ if } n = r \cdot s, \text{ then } r = 1 \text{ or } s = 1$
 - n is composite $\leftrightarrow \exists r \in \mathbb{Z}^+, \exists s \in \mathbb{Z}^+, n = r \cdot s \text{ and } r \neq 1 \text{ and } s \neq 1$
- r is rational $\leftrightarrow \exists a, b \in \mathbb{Z}, r = a/b \text{ and } b \neq 0$
- For $n, d \in \mathbb{Z}$,
 - n is divisible by $d \leftrightarrow \exists k \in \mathbb{Z}, n = dk$
- For any real number x , the floor of x , written $\lfloor x \rfloor$, is defined as follows:
 - $\lfloor x \rfloor =$ the unique integer n such that $n \leq x < n + 1$
- For any real number x , the ceiling of x , written $\lceil x \rceil$, is defined as follows:
 - $\lceil x \rceil =$ the unique integer n such that $n - 1 < x \leq n$

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

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	$A - B = A \cap B^c$	

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 **bijjective**

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

- **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 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**

Ticket Out the Door

Upcoming

Next time...

- **No class on Monday**

Reminders

- Finish Assignment 4
- Exam 2 next Wednesday!
- Office hours cancelled today
- Read 9.1 and 9.2 for next Friday
 - Write a three-sentence summary