CS1231S
AY24/25 Sem 1
by ngmh

1. Speaking Mathematically

Important Sets

- $\mathbb{N}$: the set of all natural numbers (include 0, i.e. $\mathbb{Z}_{\geq 0}$)
- $\mathbb{Z}$: the set of all integers
- $\mathbb{Q}$: the set of all rational numbers
- $\mathbb{R}$: the set of all real numbers
- $\mathbb{C}$: the set of all complex numbers

Statements

- Universal Statement $\forall$: A certain property is true for **all** elements in a set
- Conditional statement $\rightarrow$: If one thing is true then some other thing has to be true
- Existential Statement $\exists$: There is **at least one** thing for which a certain property is true
- Universal Conditional Statement
- Universal Existential Statement
- Existential Universal Statement (not the same!)

Terms used in Proofs

- Definition: Precise and unambiguous description of mathematical term.
- Axiom / Postulate: A statement that is assumed to be true without proof.
- Theorem: A mathematical statement that is proved using rigorous mathematical reasoning.
- Lemma: A small theorem; a minor result which helps to prove a theorem.
- Corollary: A result that is a simple deduction from a theorem.
- Conjecture: A statement believed to be true, but for which there is no proof (yet).

Properties of Integers on Addition and Multiplication

- Closure: $x + y \in \mathbb{Z}$
- Commutativity: $x + y = y + x$
- Associativity: $x + y + z = (x + y) + z = x + (y + z)$
- Distributivity: $x(y + z) = xy + xz$
- Trichotomy: $x = y$ or $x < y$ or $x > y$

Number Definitions

- Even and Odd Integers (Lecture 1 Slide 27): An integer is even iff $\exists k s.t. n = 2k$. An integer is odd iff $\exists k s.t. n = 2k + 1$. Every integer is even or odd, but not both (Assumption 1).
- Without Loss Of Generality (WLOG): Used before an assumption in a proof which narrows the premise to some special case, and implies that the proof for that case can be easily applied to all other cases.
- Counter-Example: Shows that a statement is not always true.
- Divisibility (Lecture 1 Slide 32): If n and d are integers with $d \neq 0$, $d \mid n$ iff $\exists k \in \mathbb{Z}$ s.t. $n = dk$
- Theorem 4.7.1: $\sqrt{2}$ is irrational
- Rational and Irrational Numbers: r is rational iff $\exists a, b \in \mathbb{Z}$ s.t. $r = \frac{a}{b}, b \neq 0$
- Fraction in lowest term (Lecture 1 Slide 37): A fraction $\frac{a}{b}$ is said to be in lowest terms if the largest integer that divides both a and b is 1. Every rational can be reduced to a fraction in its lowest term. (Assumption 2)
- Proposition 4.6.4: For all integers n, if n^2 is even then n is even. (Proof by contraposition)
- Colorful (CS1231S): An integer n is colorful if $\exists k$ s.t. $n = 3k$

2. The Logic of Compound Statements

Definitions

- Defn 2.1.1 (Statement): A statement (or proposition) is a sentence that is true or false, but not both.
- Defn 2.1.2 (Negation): The negation of p is "not p" and is denoted $\sim p$.
- Defn 2.1.3 (Conjunction): The conjunction of p and q is "p and q", denoted $p \wedge q$.
- Defn 2.1.4 (Disjunction): The disjunction of p and q is "p or q", denoted $p \vee q$.
- Defn 2.1.5 (Statement Form / Propositional Form): A statement form (or propositional form) is an expression made up of statement variables and logical connectives.
- Defn 2.1.6 (Logical Equivalence): Two statement forms are logically equivalent iff they have identical truth values for each possible substitution of statements for their statement variables. The logical equivalence of P and Q is denoted by $P \equiv Q$.
- Defn 2.1.7 (Tautology): A tautology is a statement form that is always true regardless of the truth values of its statement variables.
- Defn 2.1.8 (Contradiction): A contradiction is a statement form that is always false regardless of the truth values of its statement variables.
- Defn 2.2.1 (Conditional): The conditional of q by p is "if p then q", denoted $p \rightarrow q$. p is the hypothesis (antecedent), and q is the conclusion (consequent).
- Defn 2.2.2 (Contrapositive): The contrapositive of a conditional statement $p \rightarrow q$ is $\sim q \rightarrow \sim p$
- Defn 2.2.3 (Converse): The converse of a conditional statement $p \rightarrow q$ is $q \rightarrow p$
- Defn 2.2.4 (Inverse): The inverse of a conditional statement $p \rightarrow q$ is $\sim p \rightarrow \sim q$
- Defn 2.2.5 (Only if): "p only if q" means $\sim q \rightarrow \sim p$ or "if p then q" $p \rightarrow q$
- Defn 2.2.6 (Biconditional): The biconditional of p and q is "p if and only if q" and is denoted "$p \leftrightarrow q$"
- Defn 2.2.7 (Necessary and Sufficient Conditions): "r is a sufficient condition for s" means $r \rightarrow s$, "r is a necessary condition for s" means $s \rightarrow r$
- Defn 2.3.1 (Argument): An argument is a sequence of statements. All statements except for the final one are called premises, while the final statement is called the conclusion. The symbol $\therefore$ is normally placed before the conclusion. An argument form is valid if the conclusion is true when all the premises are true.
- Defn 2.3.2 (Sound and Unsound Arguments): an argument is sound iff it is valid and all its premises are true. An argument that is not sound is unsound.

Theorem 2.1.1 Logical Equivalences

Implication Law

$$p \rightarrow q \equiv \sim p \vee q$$

Double Negative Law

$$\sim(\sim p) \equiv p$$

Commutative Laws

$$p \wedge q \equiv q \wedge p$$
$$p \vee q \equiv q \vee p$$

Idempotent Laws

$$p \wedge p \equiv p$$
$$p \vee p \equiv p$$

Associative Laws

$$p \wedge q \wedge r \equiv (p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$$
$$p \vee q \vee r \equiv (p \vee q) \vee r \equiv p \vee (q \vee r)$$

Universal Bound Laws

$$p \vee \textbf{true} \equiv \textbf{true}$$
$$p \wedge \textbf{false} \equiv \textbf{false}$$

Distributive Laws

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$
$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

De Morgan's Laws

$$\sim(p \wedge q) \equiv \sim p \vee \sim q$$
$$\sim(p \vee q) \equiv \sim p \wedge \sim q$$

Identity Laws

$$p \wedge \textbf{true} \equiv p$$
$$p \vee \textbf{false} \equiv p$$

Absorption Laws

$$p \vee (p \wedge q) \equiv p$$
$$p \wedge (p \vee q) \equiv p$$

Negation Laws

$$p \vee \sim p \equiv \textbf{true}$$
$$p \wedge \sim p \equiv \textbf{false}$$

Negations of **true** and **false**

$$\sim\textbf{true} \equiv \textbf{false}$$
$$\sim\textbf{false} \equiv \textbf{true}$$

Argument Forms and Fallacies

- Modus Ponens:
  - If p then q
  - p
  - $\therefore q$
- Modus Tollens:
  - If p then q
  - $\sim q$
  - $\therefore \sim p$
- Generalization:
  - p
  - $p \vee q$
- Specialization:
  - $p \wedge q$
  - $\therefore p$
- Conjunction:
  - p
  - q
  - $\therefore p \wedge q$
- Elimination:
  - $p \vee q$
  - $\sim q$
  - $\therefore p$
- Transitivity:
  - $p \rightarrow q$
  - $q \rightarrow r$
  - $\therefore p \rightarrow r$
- Division into Cases
  - $p \vee q$
  - $p \rightarrow r$
  - $q \rightarrow r$
  - $\therefore r$
- Contradiction Rule
  - $\sim p \rightarrow false$
  - $\therefore p$
- Converse Error
  - $p \rightarrow q$
  - q
  - p
- Inverse Error
  - $p \rightarrow q$
  - $\sim p$
  - $\sim q$

Compund Statements Notes

- Order of Operations: $\sim, \wedge/\vee, \rightarrow / \leftrightarrow$ (use parentheses if ambiguous)
- Show logical unequivalence by (i) finding a different row in truth table, (ii) finding a counter example.
- A conditional statement is vacuously true when the hypothesis is false.
- A conditional is logically equivalent with its contrapositive, which is the negation of its converse / inverse.
- If r is a sufficient condition for s, then r is sufficient to guarantee the occurrence of r.
- If r is a necessary condition for s, s cannot occur without r.
- To test an argument form for validity, construct the truth table. A critical row is a row in the truth table in which all premises are true. If there is a critical row in which the conclusion is false, the argument form is invalid. If there are no critical rows, the argument is vacuously valid.

3. The Logic of Quantified Statements

Definitions

- Defn 3.1.1 (Predicate): A predicate is a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables. The domain of a predicate variable is the set of all values that may be substituted in place of the variable.
- Defn 3.1.2 (Truth Set): If $P(x)$ is a predicate and x has domain D, the truth set has all elements of D that make $P(x)$ true when substituted for x, denoted by $\{x \in D \mid P(x)\}$
- Defn 3.1.3 (Universal Statement): Let $Q(x)$ be a predicate and D the domain of x. A universal statement has the form $\forall x \in D, Q(x)$. A value for x for which $Q(x)$ is false is a counterexample.

- Defn 3.1.4 (Existential Statement): Let $Q(x)$ be a predicate and D the domain of x. An existential statement has the form $\exists x \in D$ s.t. $Q(x)$. The symbol $\exists!$ is used to denote uniqueness.
- Theorem 3.2.1 Negation of a Universal Statment: The negation of the statement $\forall x \in D, P(x)$ is equivalent to $\exists x \in D$ s.t. $\sim P(x)$
- Theorem 3.2.2 Negation of an Existential Statement: The negation of the statment $\exists x \in D$ s.t. $P(x)$ is equivalent to $\forall x \in D, \sim P(x)$
- Defn 3.2.1 (Contrapositive, Converse, Inverse): These terms can also be applied on universal conditional statements.
- Defn 3.2.2 (Necessary and Sufficient conditions, Only if): These terms can also be applied on universal conditional statements.
- Defn 3.4.1 (Valid Argument Form): An argument form is valid if no matter what predicates are substituted in its premises, if the premise statements are all true, then the conclusion is also true. An argument is valid iff its form is valid.

Arguments with Quantified Statements

- Universal Modus Ponens:
  - $\forall x(P(x) \to Q(x))$
  - $P(a)$ for a particular a
  - $\therefore Q(a)$
- Universal Modus Tollens
  - $\forall x, (P(x) \to Q(x)$
  - $\sim Q(a)$ for a particular a
  - $\therefore \sim P(a)$
- Universal Transitivity
  - $\forall x(P(x) \to Q(x)$
  - $\forall x(Q(x) \to R(x)$
  - $\therefore \forall x(P(x) \to R(x)$
- Universal Instantiation
  - $\forall x \in DP(x)$
  - $\therefore P(a)$ if $a \in D$
- Universal Generalisation
  - $P(a)$ for every $a \in D$
  - $\therefore \forall x \in DP(x)$
- Existential Instantiation
  - $\exists x \in DP(x)$
  - $\therefore P(a)$ for some $a \in D$
- Existential Generalisation
  - $P(a)$ for some $a \in D$
  - $\exists x \in DP(x)$
- Converse Error
  - $\forall x(P(x) \to Q(x))$
  - $Q(a)$ for a particular a
  - $\therefore P(a)$
- Inverse Error
  - $\forall x(P(x) \to Q(x))$
  - $\sim P(a)$ for a particular a
  - $\therefore \sim Q(a)$

Quantified Statements Notes

- To show a universal statement is true, we use exhaustion. To show it is false, we use a counterexample.
- To show an existential statement is true, we use an example. To show it is false, we use exhaustion.
- $\forall x \in D, Q(x) \equiv Q(x_1) \wedge Q(x_2) \wedge ... \wedge Q(x_n)$, and $\exists x \in D, Q(x) \equiv Q(x_1) \vee Q(x_2) \vee ... \vee Q(x_n)$
- Universal statements can be vacuously true if the predicate of a conditional is false for every element in the domain, which also happens if the domain is empty.
- In a statement with multiple quantifiers, the order of quantifiers with the **SAME** type can be interchanged.

4. Methods of Proof

Definitions

- Prime: An integer n is prime iff $n > 1$ and $\forall r, s$, if $n = rs$ then $r = n$ or $s = n$.
- Composite: An integer n is composite iff $n > 1$ and $\exists r, s$ s.t. $n = rs, 1 < r < n$, $1 < s < n$.
- Theorem 4.2.1: Every integer is a rational number. (Prove with $\frac{a}{1}$)
- Theorem 4.2.2: The sum of any two rational numbers is rational. (Proof by algebra)
- Corollary 4.2.3: The double of a rational number is rational.
- Theorem 4.3.1: $\forall a, b$, if $a \mid b$ then $a \leq b$ (Proof by algebra)
- Theorem 4.3.2: The only divisors of 1 are 1 and -1 (Proof by cases)
- Theorem 4.3.3: $\forall a, b, c$ if $a \mid b$ and $b \mid c$ then $a \mid c$
- Theorem 4.6.1: There is no greatest integer (Proof by contradiction)

Proofs

Methods of Proof

- Direct Proof: Show a series of steps leading from start to end. Deduction is a type of direct proof.
- Divison into Cases: Split the statement into cases and show it is true in all of them.
- Constructive Proof of Existential statements: Provide an example where the statement is true.
- Disproving Universal Statements by Counterexample: Give a counterexample where the negation is true, or where the antecedent is true and the consequent is false.
- Proving Universal Statements by Exhaustion: Show the statement is true for every element in the domain.
- Proving Universal Statements by Generalizing from the Generic Particular: Suppose x is a particular but arbitrarily chosen element of the set, show x satisfies the property.
- Proof by Contradiction:
  - Suppose the statement to be proved, S, is false. That is, the negation of the statement, $\sim S$, is true.
  - Show that this supposition leads logically to a contradiction.
  - Conclude that the statement S is true.
- Proof by Contraposition: Prove the contraposition of the statement instead.

5. Set Theory

Definitions

- Set: An **unordered** collection of objects (members / elements)
- Set-Roster Notation: Write all elements of the set between braces.
- Membership of a set: $x \in S$ means x is an element of S. Similarly, $x \notin S$ means x is not an element of S.
- Cardinality of a set: $\mid S \mid$ is the size of the set S, or the number of elements in S.
- Set-Builder Notation: Let U be a set and $P(x)$ be a predicate over U. Then the set of $x \in U$ s.t. $P(x)$ is true is $\{x \in U : P(x)\}$.
- Replacement Notation: Let A be a set and $t(x)$ be a term in a variable x. Then the set of all objects of the form $t(x)$ where $x \in A$ is $\{t(x) : x \in A\}$.
- Subset and Superset: Let A and B be sets. A is a subset of B, $A \subseteq B$, iff every element in A is also an element of B. We can also write $B \supseteq A$ or B is a superset of A.
- Proper Subset: A is a proper subset of B, $A \subsetneq B$ iff $A \subseteq B$ and $A \neq B$.
- Empty Set: $\emptyset$
- Theorem 6.2.4: An empty set is a subset of every set, $\forall A, \emptyset \subseteq A$
- Singleton: Set with exactly one element.
- Ordered Pair: An ordered pair has the form (x, y). Two Ordered pairs (a, b) and (c, d) are equal iff $a = c$ and $b = d$. This can also be extended to ordered n-tuples.
- Cartesian Product: The Cartesian product of sets A and B, $A \times B$, is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$. This can also be extended to more than 2 sets.
- Set Equality: $A = B$ iff every element of A is B and every element of B is in A, or $A \subseteq B$ and $B \subseteq A$.
- Union: The union of A and B, $A \cup B$ is the set of all elements that are in at least one of A or B.
- Intersection: The intersection of A and B, $A \cap B$ is the set of all elements that are in both A and B.
- Difference / Relative Complement: The difference of $B - A$, $B \backslash A$ is the set of elements that are in B and not A.
- Complement: The complement of A, $\bar{A}$ is the set of elemnts in U that are not in A.
- Interval Notation: $(a, b) = \{x \in \mathbb{R} : a < x < b\}$, $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$. $[]$ means closed intervals, while $()$ means open intervals.
- Disjoint: Two sets are disjoint iff they have no elements in common, $A \cap B = \emptyset$.
- Mutually / Pairwise Disjoint / Nonoverlapping: Multiple sets are mutually disjoint iff $\forall A_i, A_j$, A_i and A_j are disjoint.
- Partition: Collection of mutually disjoint sets.
- Theorem 4.4.1 Quotient-Remainder Theorem: Given n, d, $\exists! q, r$ s.t. $n = dq + r$, $0 \leq r < d$
- Power Set: $\mathcal{P}(A)$ is the set of all subsets of A. By power set axiom, any element of $\mathcal{P}(A)$ is a set.
- Theorem 6.3.1 Cardinality of Power Set of a Finite Set: If $\mid A \mid = n$, $\mid \mathcal{P}(A) \mid = 2^n$.

Set Properties

- Inclusion of Intersection: $A \cap B \subseteq A$
- Inclusion in Union: $A \subseteq A \cup B$
- Transitive Property of Subsets: $A \subseteq B \wedge B \subseteq C \to A \subseteq C$.
- Procedural Definitions: Define using $\wedge, \vee$ instead
  - $a \in X \cup Y \leftrightarrow a \in X \vee a \in Y$
  - $a \in X \cap Y \leftrightarrow a \in X \wedge a \in Y$
  - $a \in X - Y \leftrightarrow a \in X \wedge a \notin Y$
  - $a \in \bar{X} \leftrightarrow a \notin X$
  - $(a, b) \in X \times Y \leftrightarrow a \in X \wedge b \in Y$

Theorem 6.2.2 Set Identities

Commutative Laws

$$A \cup B = B \cup A$$

$$A \cap B = B \cap A$$

Associative Laws

$$(A \cup B) \cup C = A \cup (B \cup C)$$

$$(A \cap B) \cap C = A \cap (B \cap C)$$

Distributive Laws:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Identity Laws

$$A \cup \emptyset = A$$

$$A \cap U = A$$

Complement Laws

$$A \cup \bar{A} = U$$

$$A \cap \bar{A} = \emptyset$$

Double Complement Law

$$\bar{\bar{A}} = A$$

Idempotent Laws

$$A \cup A = A$$

$$A \cap A = A$$

Universal Bound Laws

$$A \cup U = U$$

$$A \cap \emptyset = \emptyset$$

De Morgan's Laws

$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$

$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$

Absorption Laws

$$A \cup (A \cap B) = A$$

$$A \cap (A \cup B) = A$$

Complements of U and $\emptyset$

$$\bar{U} = \emptyset$$

$$\bar{\emptyset} = U$$

Set Difference Law

$$A \backslash B = A \cap \bar{B}$$

6. Relations

Definitions

- Relation: A binary relation from A to B is a subset of $A \times B$. Given an ordered pair (x, y) in $A \times B$, x is related to y by R, xRy, iff $(x, y) \in R$
- Domain, Co-Domain, Range: Let R be a relation from A to B. Domain is the set $\{a \in A : aRb$ for some $b \in B\}$. Co-Domain is B. Range is the set $\{b \in B : aRb$ for some $a \in A\}$

- Inverse Relation: The inverse relation R^{-1} is $\{(y,x) \in B \times A : (x,y) \in R\}$
- Relation on a Set: A relation on a set A is a subset of $A \times A$.
- Composite Relations: Let $R \subseteq A \times B$ and $S \subseteq B \times C$ be relations. The composition of R with S, denoted $S \circ R$ is the relation from A to C s.t. $\forall x \in A, \forall Z \in C, xS \circ Rz \leftrightarrow (\exists y \in B, xRy \land ySz)$.
- Proposition: Composition is Associative
- Proposition: Inverse of Composition: $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.
- n-ary Relation: Subset of A^n
- Reflexivity: R is reflexive iff $\forall x \in A, xRx$.
- Symmetry: R is symmetric iff $\forall x, y \in A, xRy \to yRx$
- Antisymmetry: R is antisymmetric iff $\forall x, y \in A, xRy \land yRx \to x = y$.
- Assymetry: R is asymmetric iff $\forall x, y \in A, xRy \to y \not R x$
- Transitivity: R is transitive iff $\forall x, y, z \in A, xRy \land yRz \to xRz$.
- Transitive Closure: The transitive closure of R on A is R^t on A s.t. (i) R^t is transitive, (ii) $R \subseteq R^t$, (iii) If S is another transitive relation containing R, $R^t \supseteq S$. Reflexive and Symmetric closure are similarly defined.
- Partition: $\mathscr{C}$ is a partition of A if (i) $\mathscr{C}$ is a set where all elements are non-empty subsets of A, (ii) Every element of A is in exactly one element of $\mathscr{C}$. Elements of a partition are components. Alternatively, $\forall x \in A, \exists! S \in \mathscr{C}(x \in S)$.
- Relation Induced by Partition: The relation R induced by a partition on A is $\forall x, y, \in A, xRy \leftrightarrow \exists$ a component S of $\mathscr{C}$ s.t. $x, y, \in S$.
- Theorem 8.3.1 Relation Induced by a Partition: R is reflexive, symmetric, and transitive.
- Equivalence Relation: R is an equivalence relation iff R is reflexive, symmetric and transitive. The symbol $\sim$ is commonly used.
- Equivalence Class: Suppose A is a set and $\sim$ is an equivalence relation on A. For each $a \in A$, the equivalence class of a, $[a]$, is the set of elements $x \in A$ s.t. $a \sim x$. $[a]_\sim = \{x \in A : a \sim x\}$
- Theorem 8.3.4: The partition Induced by an Equivalence Relation: If R is an equivalence relation on A, then the distinct equivalence classes of R form a partition of A.
- Congruence: a is congruent to b modulo n iff $a - b = nk$ for some $k \in \mathbb{Z}$.
- Congruence mod n is an equivalence relation on $\mathbb{Z}$ for every $n \in \mathbb{Z}^+$
- Set of equivalence classes: $A/\sim$ is the set of all equivalence classes with respect to $\sim$, $A/\sim = \{[x]_\sim : x \in A\}$.
- Partial Order Relation: R is a partial order iff R is reflexive, antisymmetric and transitive.
- Partially Ordered Set: A is a poset with respect to a partial order relation R on A, (A, R).
- Curly Less Than Equals: $\preccurlyeq$ is used for partial orders to prevent confusion with $\leq$.
- Hasse Diagrams: Simplification of the directed graph of a partial order relation. Place vertices s.t. all arrows point upwards, then remove all self-loops, remove arrows implied by transitivity, and remove direction indicators.
- Comparable: a and b are comparable iff $a \preccurlyeq b$ or $b \preccurlyeq a$. If not, they are noncomparable.
- Compatible: a and b are compatible iff $\exists c \in A, a \preccurlyeq c, b \preccurlyeq c$. (There are other possible definitions, be careful.)
- Maximal Element: c is maximal iff $\forall x \in A, c \preccurlyeq x \to c = x$.
- Minimal Element: c is minimal iff $\forall x \in A, x \preccurlyeq c \to c = x$.
- Largest Element: c is the largest iff $\forall x \in A, x \preccurlyeq c$.
- Smallest Element: c is the smallest iff $\forall x \in A, c \preccurlyeq x$.
- Total Order Relations: R is a total order relation if R is a partial order and $\forall x, y \in A, xRy \lor yRx$.
- Linearization: A total order s.t. $x \preccurlyeq y \to x \preccurlyeq^* y$.
- Well-Ordered Set: A is well-ordered iff every non-empty subset of A contains a smallest (not minimal) element.

Lemma Rel.1 Equivalence Classes

The following are equivalent:

- (i) $x \sim y$
- (ii) $[x] = [y]$
- (iii) $[x] \cap [y] \neq \emptyset$

Proof

- (i) $\to (ii)$
  - Suppose $x \sim y$
  - $y \sim x$ by symmetry
  - For every $z \in [x]$
  - $x \sim z$ by definition of $[x]$
  - $y \sim z$ by transitivity
  - $z \in [y]$ by definition of $[y]$
  - $\therefore [x] \subseteq [y]$
  - Similarly for $[y] \subseteq [x]$
  - $\therefore [x] = [y]$
- (ii) $\to$ (iii)
  - Suppose $[x] = [y]$
  - $[x] \cap [y] = [x]$ by Idempotent Law
  - However, $x \sim x$ by reflexivity
  - This shows $x \in [x] = [x] \cap [y]$
  - $\therefore [x] \cap [y] \neq \emptyset$
- (iii) $\to$ (i)
  - Suppose $[x] \cap [y] \neq \emptyset$
  - Take $z \in [x] \cap [y]$
  - Then $z \in [x] and z \in [y]$ by definition of $\cap$
  - Then $x \sim z$ and $y \sim z$ by definition of $[x]$ and $[y]$
  - $y \sim z$ implies $z \sim y$ by symmetry
  - $\therefore x \sim y$ by transitivity

Theorem Rel.2 Equivalence classes form a partition

$A/\sim$ is a partition of A Proof Steps

- $A/\sim$ is a set by definition
- Show every element of $A/\sim$ is a nonempty subset of A.
  - Let $S \in A/\sim$
  - Find $x \in A$ s.t. $S = [x]$ by definition of $A/\sim$
  - Then $S = [x] \subseteq A$ by definition of equivalence classes
  - $x \sim x$ by reflexivity of $\sim$
  - Hence $x \in [x] = S$ by definition of $[x]$
  - $\therefore S$ is non-empty
- Show every element of A is in at least one element of $A/\sim$.
  - Let $x \in A$
  - $x \sim x$ by reflexivity of $\sim$
  - $\therefore x \in [x] \in A/\sim$
- Show every element of A is in at most one element of $A/\sim$.
  - Let $x \in A$ s.t. $x \in S_1, x \in S_2$
  - Find $y_1, y_2 \in A$ s.t. $S_1 = [y_1]$ and $S_2 = [y_2]$
  - $x \in [y_1] \cap [y_2]$
  - $[y_1] \cap [y_2] \neq \emptyset$
  - $\therefore S_1 = [y_1] = [y_2] = S_2$ by equivalence classes lemma

Relations Notes

- Relations can be represented with arrow diagrams or directed graphs.
- Composite relations can be found by walking on the directed graph.
- We can view partitions as a "in the same component" relation.
- Properties such as reflexivity and symmetry can be vacuously true. A set can be both symmetric and antisymmetric at the same time.
- Any smallest element is minimal, and any largest element is maximal.
- Kahn's Algorithm
  - Find a minimal element c of A
  - Remove c from A and add it to the linearization
  - Repeat until A is empty

Useful Tutorial Questions

- Tutorial 1 Question 10: The product of any two odd integers is an odd integer.
- Tutorial 1 Question 11: n^2 is odd iff n is odd. n^2 is even iff n is even.
- Tutorial 2 Question 4: Rational numbers are closed under addition. Integers and rational numbers are not closed under division.
- Tutorial 2 Question 11: If $n = ab$ where a and b are positive, then $a \leq n^{\frac{1}{2}}$ or $b \leq n^{\frac{1}{2}}$.
- Tutorial 3 Question 5: $A \cap (B \backslash C) = (A \cap B) \backslash C$.
- Tutorial 3 Question 6: $A \backslash (B \backslash C) = (A \backslash B) \cup (A \cap C)$.
- Tutorial 3 Question 8: $A \subseteq B$ iff $A \cup B = B$.
- Tutorial 3 Question 9: $(A \backslash B) \cup (B \backslash A) = (A \cup B) \backslash (A \cap B)$.
- Tutorial 4 Question 2: Show the following are logically equivalent: (i) R is symmetric, (ii) $\forall x, y \in A, xRy \leftrightarrow yRx$, (iii) $R = R^{-1}$.
  - (i) $\to$ (ii)
    - Suppose R is symmetric
    - Let $x, y \in A$
    - If xRy then yRx by symmetry of R
    - If yRx then xRy by symmetry of R
    - $\therefore xRy \leftrightarrow yRx$
  - (ii) $\to$ (iii)
    - Suppose $\forall x, y \in A, xRy \leftrightarrow yRx$
    - $\forall x, y \in A$
    - $(x, y) \in R \leftrightarrow xRy$ by definition of xRy
    - $\leftrightarrow yRx$
    - $\leftrightarrow xR^{-1}y$ by definition of R^{-1}
    - $\leftrightarrow (x, y) \in R^{-1}$ by definition of $xR^{-1}y$
    - $\therefore R = R^{-1}$
  - (iii) $\to$ (i)
    - Suppose $R = R^{-1}$
    - Let $x, y \in A, xRy$
    - Then $xR^{-1}y$ as $R = R^{-1}$
    - yRx by definition of R^{-1}
    - $\therefore$ R is symmetric
- Tutorial 4 Question 5: For an equivalence relation R,
  - (i) $R^{-1} \circ R = R \circ R^{-1}$
  - (ii) $R \subseteq R \circ R$
  - (iii) $R \circ R \subseteq R$
  - (iv) $R \circ R^{-1} = R$
  - (v) $R = R \circ R$ from (ii) and (iii)
- Tutorial 4 Question 7: Composition of relations is associative, $T \circ (S \circ R) = (T \circ S) \circ R$.
- Tutorial 5 Question 5: $\subseteq$ on $\mathcal{P}(A)$ is a partial order.
- Tutorial 5 Question 8: Every asymmetric relation is antisymmetric.
- Tutorial 5 Question 11: Any two comparable elements are compatible. Any two compatible elements are not necessarily compatible.

pls give me A+ prof thanks