Logic

Basic Notations

- $\mathbb{R}$ set of real numbers
- $\mathbb{Z}$ set of integers (includes 0)
- $\mathbb{Q}$ set of rational numbers
- $\mathbb{N}$ set of natural numbers (includes 0)
- $\exists$ there exists...
- $\exists!$ there exists a unique...
- $\forall$ for all...
- $\in$ member of...
- s.t. such that...
- $\rightarrow$ if...then…
- $\leftrightarrow$ if, and only if/iff

Note: 0 is neither positive nor negative

Definition 2.1.1 (Statement)
A statement (or proposition) is a sentence that is true or false, but not both.

Definition 2.1.2 (Negation)
If p is a statement variable, the negation of p is "not p" or "it is not the case that p" and is denoted ~p.

Definition 2.1.3 (Conjunction)
If p and q are statement variables, the conjunction of p and q is "p and q", denoted p ∧ q.

Definition 2.1.4 (Disjunction)
If p and q are statement variables, the disjunction of p and q is "p or q", denoted p ∨ q.

Definition 2.1.5 (Statement Form/Propositional Form)
A statement form (or propositional form) is an expression made up of statement variables and logical connectives that becomes a statement when actual statements are substituted for the component statement variables.

Definition 2.1.6 (Logical Equivalence)
Two statement forms are called logically equivalent if, and only if, they have identical truth values for each possible substitution of statements for their statement variables. The logical equivalence of statement forms P and Q is denoted by P ≡ Q.

Exclusive-Or
Denoted as p XOR q or p $\oplus$ q. Statement will only be true if only one of the variable is true

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

Definition 2.1.7 (Tautology)
A tautology is a statement form that is always true regardless of the truth values of the individual statements substituted for its statement variables.

Definition 2.1.8 (Contradiction)
A contradiction is a statement form that is always false regardless of the truth values of the individual statements substituted for its statement variables.

Definition 2.2.1 (Conditional)
If p and q are statement variables, the conditional of q by p is "if p then q" or "p implies q", denoted p → q. It is false when p is true and q is false; otherwise, it is true. We called p the hypothesis (or antecedent) and q the conclusion (or consequent).

A conditional statement that is true because its hypothesis is false is called *vacuously true* or *true by default.*

Definition 2.2.2 (Contrapositive)
The contrapositive of p → q is ~q → ~p.

Definition 2.2.3 (Converse)
The converse of p → q is q → p.

Definition 2.2.4 (Inverse)
The inverse of p → q is ~p → ~q.

Equivalence

(Conditional) p → q ≡ ~q → ~p (Contrapositive)

(Converse) p → q ≡ ~p → ~q (Inverse)

Definition 2.2.5 (Only If)
If p and q are statements, "p only if q" means "if not q then not p" or "$\sim q \rightarrow \sim p$" Or, equivalently, "if p then q" or "$p \rightarrow q$"
Note: "p if q" means "if q then p" or "$q \rightarrow p$"

Definition 2.2.6 (Biconditional)
Given statement variables p and q, the biconditional of p and q is denoted p ↔ q. It is true if both p and q have the same truth values and is false if p and q have opposite truth values

Definition 2.2.7 (Necessary & Sufficient Conditions)
If r and s are statements,
"r is a sufficient condition for s" means "if r then s" or "$r \rightarrow s$"

"r is a necessary condition for s" means "if not r then not s" or "if s then r" or "$s \rightarrow r$"

Order of Operations
First: ~ (also represented as ~).
No priority between ∧ and ∨

p ∧ q ∨ r is ambiguous

(p ∧ q) ∨ r or p ∧ (q ∨ r) is clear

Last: the implication, →. Can be overwritten by parenthesis

Theorem 2.1.1 (Logical Equivalences)

Commutative Laws
$$p \wedge q \equiv q \wedge p$$
$$p \vee q \equiv q \vee p$$
Associative Laws
$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$$
$$(p \vee q) \vee r \equiv p \vee (q \vee r)$$
Distributive Laws
$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$
$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$
Identity Laws
$$p \wedge true \equiv p$$
$$p \vee false \equiv p$$
Negation Laws
$$p \vee \sim p \equiv true$$
$$p \wedge \sim p \equiv false$$
Double Negative Law
$$\sim(\sim p) \equiv p$$
Idempotent Laws
$$p \wedge p \equiv p$$
$$p \vee p \equiv p$$
Universal Bound Laws
$$p \vee true \equiv true$$
$$p \wedge false \equiv false$$
De Morgan's Laws
$$\sim(p \wedge q) \equiv \sim p \vee \sim q$$
$$\sim(p \vee q) \equiv \sim p \wedge \sim q$$
Absorption Laws
$$p \vee (p \wedge q) \equiv p$$
$$p \wedge (p \vee q) \equiv p$$
Negations of true and false
$$\sim true \equiv false$$
$$\sim false \equiv true$$

Implication Law (Not under Theorem 2.1.1)
$$p \rightarrow q \equiv \sim p \vee q$$
$$\sim(p \rightarrow q) \equiv p \wedge \sim q$$

Definition 2.3.1 (Argument)
An argument (argument form) is a sequence of statements (statement forms). All statements in an argument (argument form), except for the final one, are called premises (or assumptions or hypothesis). The final statement (statement form) is called the conclusion. The symbol $\cdot$ / ∴ , which is read "therefore", is normally placed just before the conclusion.

To say that an argument form is **valid** means that no matter what particular statements are substituted for the statement variables in its premises, if the resulting premises are all true, then the conclusion is also true.

Definition 2.3.2 (Sound and Unsound Arguments)
An argument is called sound if, and only if, it is valid, and all its premises are true. An argument that is not sound is called unsound.

Rules of Inference

Modus ponens
$$p \rightarrow q$$
$$p$$
$$\cdot\, q$$
Modus tollens
$$p \rightarrow q$$
$$\sim q$$
$$\cdot\, \sim p$$
Generalization
$$P$$
$$\cdot\, p \vee q$$
Specialization
$$p \wedge q$$
$$\cdot\, p$$
Elimination
$$p \vee q$$
$$\sim q$$
$$\cdot\, p$$
Transitivity
$$p \rightarrow q$$
$$q \rightarrow r$$
$$\cdot\, p \rightarrow r$$
Proof by Division into Cases
$$p \vee q$$
$$p \rightarrow r$$
$$q \rightarrow r$$
$$\cdot\, r$$
Contradiction Rule
$$\sim p \rightarrow false$$
$$\cdot\, p$$

Fallacies

Converse Error
$$p \rightarrow q$$
$$q$$
$$\cdot\, p$$
Inverse Error
$$p \rightarrow q$$
$$\sim p$$
$$\cdot\, \sim q$$
False premise
- Valid but unsound argument as premise is false

Definition 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.

Definition 3.1.2 (Truth set)
If P(x) is a predicate and x has domain D, the truth set is the set of all elements of D that make P(x) true when they are substituted for x. The truth set of P(x) is denoted {x ∈ D | P(x)}.

Definition 3.1.3 (Universal Statement)
Let Q(x) be a predicate and D the domain of x. A universal statement is a statement of the form

$$\forall x \in D, Q(x)$$

It is defined to be true iff Q(x) is true for every x in D. It is defined to be false iff Q(x) is false for at least one x in D.
A value for x for which Q(x) is false is called a counterexample.

Definition 3.1.4 (Existential Statement)
Let Q(x) be a predicate and D the domain of x. An existential statement is a statement of the form

$$\exists x \in D\ s.t. Q(x)$$

It is defined to be true iff Q(x) is true for at least one x in D. It is defined to be false iff Q(x) is false for all x in D.

Theorem 3.2.1 (Negation of Universal State.)
The negation of a statement of the form

$$\forall x \in D, P(x)$$

is logically equivalent to a statement of the form

$$\exists x \in D\ s.t. \sim P(x)$$

Theorem 3.2.2 (Negation of Existential State.)
The negation of a statement of the form

$$\exists x \in D\ s.t. P\ (x)$$

is logically equivalent to a statement of the form

$$\forall x \in D, \sim P(x)$$

Definition 3.2.1 (Contrapositive, converse, inverse of Universal Conditonal State.)
Same as conditional statements

Definition 3.2.2 (Necessary and Sufficient conditions, Only if of Universal Conditional State.)
Same as Conditional Statements

Vacuously True
Can be applied to conditional statements, universal conditional statements and universal statements
- statements are vacuously true iff hypothesis is false/predicate, P(x) is false for every x ∈ D (or D is empty)

Universal & Existential General Rule
'All boys wear glasses' is written as

$$\forall x(Boy(x) \rightarrow Glasses(x))$$

If conjunction was used, this statement would be falsified by the existence of a 'non-boy' in the domain of x.

'There is a boy who wears glasses' is written as

$$\exists x(Boy(x) \land Glasses(x))$$

If implication was used, this statement would true even if the domain of x is empty.

Multiply-Quantified Statements
To establish the truth of statements:

$$\forall x \in D, \exists y \in E\ s.t. P(x, y)$$

Given any x in D, find a y in E that works for that particular x

$$\exists x \in D\ s.t. \forall y \in E, P(x, y)$$

Find a particular x in D that will work for any y in E

Negation of Multiply-Quantified Statements

$$\sim (\forall x \in D, \exists y \in E\ s.t. P(x, y))$$
$$\equiv$$
$$\exists x \in D\ s.t. \forall y \in E, \sim P(x, y)$$

Order of Quantifiers
Order matters if quantifiers are different e.g., both ∀ and ∃. Order doesn't matter if all quantifiers are the same

Implicit Quantification
The notation $P(x) \rightarrow Q(x)$ means that every element in the truth set of P(x) is in the truth set of Q(x), or equivalently, $\forall x, P(x) \rightarrow Q(x)$.
The notation $P(x) \leftrightarrow Q(x)$ means that P (x) and Q(x) have identical truth sets, or equivalently, $\forall x, P\ (x) \leftrightarrow Q(x)$

Universal Instantiation
If some property is true of everything in a set, then it is true of any particular thing in the set.

Rules of Inference for Quantified Statements
Universal Modus ponens

$$\forall x \in D, (P(x) \rightarrow Q(x))$$
$$P(a)\ for\ particular\ a \in D$$
$$\cdot\ Q(a)$$

Universal Modus tollens

$$\forall x \in D, (P(x) \rightarrow Q(x))$$
$$\sim Q(a)\ for\ particular\ a \in D$$
$$\cdot \sim P(a)$$

Universal Transitivity

$$\forall x\ (P(x) \rightarrow Q(x))$$
$$\forall x\ (Q(x) \rightarrow R(x))$$
$$\cdot\ \forall x\ (P(x) \rightarrow R(x))$$

Universal Instantiation

$$\forall x \in D, P(x)$$
$$\cdot\ P(a)\ if\ a \in D$$

Universal Generalisation

$$P(a)\ for\ every\ a \in D$$
$$\cdot\ \forall x \in D, P(x)$$

Existential Instantiation

$$\exists x \in D, P(x)$$
$$\cdot\ P(a)\ if\ a \in D$$

Existential Generalisation

$$P(a)\ for\ some\ a \in D$$
$$\cdot\ \exists x \in D, P(x)$$

Definition 3.4.1 (Valid Argument Form)
To say that an argument form is valid means the following: No matter what particular predicates are substituted for the predicate symbols in its premises, if the resulting premise statements are all true, then the conclusion is also true. An argument is called valid if, and only if, its form is valid.

Valid Arguments as Tautologies
All valid arguments can be restated as tautologies.

Additional Notes (Valid Argument as Tautology)
Given an argument:

$$p1$$
$$p2$$
$$\vdots$$
$$pk$$
$$\therefore q$$

where $p1, p2, \dots, pk$ are the k premises and q the conclusion, we can say that "the argument is valid if and only if $(p1 \land p2 \land \cdots \land pk) \longrightarrow q$ is a tautology"

Proving Valid Arguments
- by truth table, where all critical rows' (row where all premises are true) conclusion is true
- by proving the argument is a tautology
  - rearrange into a conditional statement
- proof by contradiction
  1. premises arise to contradiction, hence argument vacuously valid
  2. assume argument is invalid (take conclusion as false), if contradiction arise, argument is valid

You can utilize rules of inference, conjunction of premises to arrive at conclusion
- as you are assuming all premises to be true to check if conclusion is also true

Set Theory

Set

- unordered collection of elements
- order and duplicates do not matter

Set-Roster Notation

A set may be specified by writing all of its elements between braces e.g., {2,3,4}, {1,2,3,...}

Set-Builder Notation (members that fulfil predicate)

Let U be a set and $P(x)$ be a **predicate** over U. Then the set of all elements $x \in U$ such that $P(x)$ is true is denoted

$$\{x \in U : P(x)\} \text{ or } \{x \in U \mid P(x)\}$$

Replacement Notation (apply term on members)

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 ranges over the elements of A is denoted

$$\{t(x) : x \in A\} \text{ or } \{t(x) \mid x \in A\}$$

Definition: Membership of a Set (Notation: ∈)

If S is a set, the notation $x \in S$ means that x is an element of S. ($x \notin S$ means x is not an element of S.)

Definition: Cardinality of a Set (Notation: $|S|$)

The cardinality of a set S, denoted as $|S|$, is the size of the set, that is, the number of elements in S.

Definition: Subsets & Superset

A is a subset of B, written $A \subseteq B$, iff every element of A is also an element of B. Symbolically,

$$A \subseteq B \Leftrightarrow \forall x(x \in A \rightarrow x \in B)$$

Definition: Proper Subset

Let A and B be sets. A is a proper subset of B, denoted $A \subsetneq B$, iff $A \subseteq B$ and $A \neq B$. In this case, we may say that the inclusion of A in B is proper or strict

Definition: Empty Set

An empty set has no element and is denoted $\emptyset$

Definition: Set Equality

Given sets A and B, A equals B, written $\boldsymbol{A} = \boldsymbol{B}$ iff every element of A is in B and every element of B is in A. Symbolically:

$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A.$$

Or from definition of subsets:

$$A = B \Leftrightarrow \forall x\ (x \in A \Leftrightarrow x \in B)$$

Proving Set Equality (A=B)

- Prove A is a subset of B ($x \in A \Rightarrow x \in B$)
- Prove B is a subset of A ($x \in B \Rightarrow x \in A$)

Definition: Union (in A or B)

$$A \cup B = \{x \in U : x \in A \vee x \in B\}$$

Definition: Intersection (in A and B)

$$A \cap B = \{x \in U : x \in A \wedge x \in B\}$$

Definition: Set difference (in B not in A)

$$B \backslash A = \{x \in U : x \in B \wedge x \notin A\}$$

Definition Set complement (not in A)

$$\bar{A} = \{x \in U \mid x \notin A\}$$

Definition (Power Sets)

Given a set A, the power set of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A

For example,

$$let\ A = \{x, y\}$$
$$\mathcal{P}(A) = \{\phi, \{x\}, \{y\}, \{x, y\}\}$$

Definition: Disjoint (no elements in common)

A and B are disjoint iff $A \cap B = \emptyset$

Definition: Mutually Disjoint

Sets $A_1, A_2, A_3, \cdots$ are mutually disjoint (or pairwise disjoint or nonoverlapping) iff no two sets A_i and A_j with distinct subscripts have any elements in common,

$$\forall i, j \in \{1,2,3,\ldots\},\ i \neq j \rightarrow A_i \cap A_j = \emptyset$$

Unions and Intersections of an Indexed Collection of Sets

Given sets A_0, A_1, A_2 ... that are subsets of a universal set U and a given nonnegative integer n,

$$\bigcup_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ for at least one } i = 0, 1, 2, \ldots, n\}$$

$$\bigcup_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for at least one non -ve integer } i\}$$

$$\bigcap_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ for all } i = 0, 1, 2, \ldots, n\}$$

$$\bigcap_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for all non -ve integer } i\}$$

Definition: Ordered Pair

An ordered pair is an expression of the form (x, y). Two ordered pairs (a, b) and (c, d) are equal iff $a = c$ and $b = d$. Symbolically:

$$(a, b) = (c, d) \Leftrightarrow (a = c) \wedge (b = d)$$

Definition: Ordered n-tuples

Let $n \in \mathbb{Z}^+$ and let $x_1, x_2, \cdots, x_n$ be (not necessarily distinct) elements. An ordered $\boldsymbol{n}$-tuple is an expression of the form $(x_1, x_2, \cdots, x_n)$

$$(x_1, x_2, \cdots, x_n) = (y_1, y_2, \cdots, y_n)$$
$$\Leftrightarrow x_1 = y_1, x_2 = y_2, \cdots, xn = yn$$

Definition: Cartesian Product

Given sets A and B, the Cartesian product of A and B, denoted $\boldsymbol{A} \times \boldsymbol{B}$, is the set of all ordered pairs (a, b) where a is in A and b is in B. Symbolically:

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

For example,

{1, 2, 3} × {a, b} =
{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)}

Definition: Generalised Cartesian Product

Given sets $A_1, A_2, \cdots, A_n$,

$$A_1 \times A_2 \times \cdots \times A_n =$$
$$\{a_1, a_2, \cdots, a_n : a_1 \in A_1 \wedge a_2 \in A_2 \wedge \cdots \wedge a_n \in A_n\}$$

If A is a set, then $A^n = A \times A \times \cdots \times A$ (n times)

Procedural Versions of Set Definitions

Let X and Y be subsets of a universal set U and suppose a and b are elements of U.

1. $a \in X \cup Y \Leftrightarrow a \in X \vee a \in Y$
2. $a \in X \cap Y \Leftrightarrow a \in X \wedge a \in Y$
3. $a \in X - Y \Leftrightarrow a \in X \wedge a \notin Y$
4. $a \in \bar{X} \Leftrightarrow a \notin X$
5. $(a, b) \in X \times Y \Leftrightarrow a \in X \wedge b \in Y$

Note: In a context where U is the universal set (so that implicitly means $U \supseteq X$), the complement of X, denoted $\bar{X}$,is defined by $\bar{X} = U \setminus X$.

Theorem 6.2.4 (Empty set subset of all sets)

An empty set is a subset of all sets.

$$\forall A, A\ is\ a\ set, \emptyset \subseteq A$$

Theorem (Cardinality of Power Set of a Finite Set)

Let A be a finite set where $|A| = n$, then $|\mathcal{P}(A)| = 2^n$

Theorem 6.3.1

Suppose A is a finite set with n elements, then $\mathcal{P}(A)$ has 2^n elements. In other words, $\mathcal{P}\ A = 2^{|A|}$.

Theorem 6.2.1 (Some subset relations)

Inclusion of Intersection

$$A \cap B \subseteq A$$
$$A \cap B \subseteq B$$

Inclusion in Union

$$A \subseteq A \cup B$$
$$B \subseteq A \cup B$$

Transitive Property of Subsets

$$A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$$

Theorem 6.2.2 (Set Identities)

Let all sets referred to below be subsets of a universal set U. ~ is used in replacement of set complement

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

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

Proving Subsets (A ⊆ B)

- let x ∈ A
- then show x ∈ B

Relations

Definition: Relation
Let A and B be sets. A (binary) relation from $\boldsymbol{A}$ to $\boldsymbol{B}$ is a subset of $\boldsymbol{A} \times \boldsymbol{B}$.

$$x\ R\ y \text{ means } (x, y) \in R$$
$$x \not R\ y \text{ means } (x, y) \notin R$$

Definitions: Domain, Co-domain, Range
Let A and B be sets and R be a relation from A to B.
The domain of R,
$$Dom(R) = \{a \in A : aRb \text{ for some } b \in B\}$$
The co-domain of R,
$$coDom(R) = B.$$
The range of R,
$$Range(R) = \{b \in B : aRb \text{ for some } a \in A\}$$

Definition: Inverse of a Relation
Let R be a relation from A to B. Define the inverse relation R^{-1} from B to A as follows:
$$R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\}$$
or
$$\forall x \in A, \forall y \in B\ (\ (y, x) \in R^{-1} \Leftrightarrow (x, y) \in R)$$
Also, $\forall x \in A, \forall y \in B\ (yR^{-1}x \Leftrightarrow xRy)$

Definition: Relation on a Set
A relation on a set $\boldsymbol{A}$ is a relation from A to A. In other words, a relation on a set A is a subset of $A \times A$

Definition: n-ary Relation
Given n sets $A_1, A_2, \cdots, A_n$, an $\boldsymbol{n}$-ary relation $\boldsymbol{R}$ on $A_1 \times A_2 \times \cdots \times A_n$ is a subset of $A_1 \times A_2 \times \cdots \times A_n$

Definition: Composition of Relations
Let A, B and C be sets. Let $R \subseteq A \times B$ be a relation. Let $S \subseteq B \times C$ be a relation. The composition of R with S, denoted $S \circ R$, is the relation from A to C such that:
$$\forall x \in A, \forall z \in C\ (x\ S \circ R\ z \Leftrightarrow (\exists y \in B\ (xRy \wedge ySz)\ )\ )$$

Proposition: Composition is Associative
Let A, B, C, D be sets. Let $R \subseteq A \times B$, $S \subseteq B \times C$ and $T \subseteq C \times D$ be relations.
$$T \circ (S \circ R) = (T \circ S) \circ R = T \circ S \circ R$$

T4

Proposition: Inverse of Composition
Let A, B and C be sets. Let $R \subseteq A \times B$ and $S \subseteq B \times C$ be relations.
$$(S \circ R)^{-1} = R^{-1} \circ S^{-1}$$

Definitions: Reflexivity
R is reflexive iff $\forall x \in A\ (xRx)$

Definition: Symmetry
R is symmetric iff $\forall x, y \in A\ (xRy \Rightarrow yRx)$

Definition: Transitivity
R is transitive iff $\forall x, y, z \in A\ (xRy \wedge yRz \Rightarrow xRz)$

Definition: Antisymmetry
Let R be a relation on a set A. R is antisymmetric iff
$$\forall x, y \in A\ (x\ R\ y \wedge y\ R\ x \Rightarrow x = y)$$
Note: antisymmetry $\not\equiv$ non-symmetry

Definition: Asymmetry (Tutorial 5)
R is asymmetric iff $\forall x, y \in A\ (x\ R\ y \Rightarrow y \not R\ x)$

Definition: Transitive Closure
Let A be a set and R a relation on A. The transitive closure of R is the relation R^t on A that satisfies the following three properties:

1. R^t is transitive
2. $R \subseteq R^t$
3. If S is any other transitive relation that contains R, then $R^t \subseteq$

Intuitively, can be understood as the relation obtained by adding the least number of ordered pairs to ensure transitivity

Reflexive Closure (Tutorial 5 Q5)
The reflexive closure S of a relation R on a set A is obtained by adding (a, a) to R for each a ∈ A.
Symbolically, $S = R \cup \{(x, x) : x \in X\}$.

Definition: Partition
C is a partition of a set A if the following hold:
(1) C is a set of which all elements are non-empty subsets of A,
$$\emptyset \neq S \subseteq A \text{ for all } S \in C$$
(2) Every element of A is in exactly one element of C,
$$\forall x \in A\ \exists S \in C\ (x \in S) \text{ and}$$
$$\forall x \in A\ \forall S_1, S_2 \in C\ (x \in S_1 \wedge x \in S_2 \Rightarrow S_1 = S_2)$$

Or simply,
$$\forall x \in A\ \exists!\ S \in C\ (x \in S)$$
Elements of a partition are called components

In layman's, a partition of a set A is a finite or infinite collection of nonempty, mutually disjoint subsets whose union is A (every element of A is in exactly one component of C)

Definition: Relation Induced by a Partition
Given a partition C of a set A, the relation R induced by the partition is defined on A as follows:
$$\forall x, y \in A,\ xRy \Leftrightarrow \exists \text{ a component } S \text{ of C s.t. } x, y \in S$$

Definition: Equivalence Relation
Let A be a set and R a relation on A. R is an equivalence relation iff R is reflexive, symmetric and transitive

Definition: Equivalence Class
Suppose A is a set and ~ is an equivalence relation on A. For each $a \in A$, the equivalence class of a, denoted $[\boldsymbol{a}]$ is the set of all elements $x \in A$ s.t. a is ~-related to x.
Symbolically,
$$[a]_{\sim} = \{x \in A : a{\sim}x\}$$

Definition: Set of equivalence classes (≡ partition)
Let A be a set and ~ be an equivalence relation on A. Denote by $A/{\sim}$ the set of all equivalence classes with respect to ~,
$$A/{\sim} = \{[x]_{\sim} : x \in A\}$$

Definition: Congruence
Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Then a is congruent to b modulo n iff $a - b = nk$ for some $k \in \mathbb{Z}$. Symbolically
$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b)$$

Proposition (Lecture 6 Slide 54)
Congruence-mod n is an equivalence relation on $\mathbb{Z}$ for every $n \in \mathbb{Z}+$.

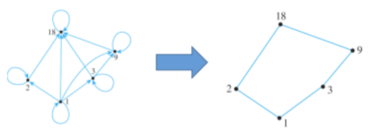
Definition: Partial Order Relation
Let R be a relation on a set A. Then R is a partial order relation (or simply partial order) denoted using $\preccurlyeq$ iff R is reflexive, antisymmetric and transitive

Definition: Partially Ordered Set
A set A is called a partially ordered set (or poset) with respect to a partial order relation R on A, denoted by (A, R)

Definition: Hasse Diagram
Let $\preccurlyeq$ be a partial order on a set A. A Hasse diagram of $\preccurlyeq$ satisfies the following condition for all distinct x, y, $m \in A$:
If $x \preccurlyeq y$ and no $m \in A$ is such that $x \preccurlyeq m \preccurlyeq y$, then x is placed below y with a line joining them, else no line joins x and y.

Hasse Diagrams
The Hasse diagram is a simplified directed graph.

1. Draw the directed graph so that all arrows point upwards.
2. Eliminate all self-loops.
3. Eliminate all arrows implied by transitivity.
4. Remove the direction of the arrows.



Directed graph of the "divides" relation on {1,2,3,9,18}

Hasse diagram of the "divides" relation on {1,2,3,9,18}

Definition: Comparability
Suppose $\preccurlyeq$ is a partial order relation on a set A. Elements a and b of A are said to be comparable iff either $a \preccurlyeq b$ or $b \preccurlyeq a$. Otherwise, a and b are noncomparable

Definition: Compatible
Elements a, b are compatible iff there exists c ∈ A such that a ≤ c and b ≤ c.

Definition: Maximal
Let $\preccurlyeq$ be a partial order on the set A and $c \in A$. c is a maximal element of A iff
$$\forall x \in A\ (c \preccurlyeq x \Rightarrow c = x)$$

Definition: Largest/Maximum
Let $\preccurlyeq$ be a partial order on the set A and $c \in A$. c is the largest element of A iff
$$\forall x \in A\ (x \preccurlyeq c)$$

Definition: Minimal
Let $\preccurlyeq$ be a partial order on the set A and $c \in A$. c is a minimal element of A iff
$$\forall x \in A\ (x \preccurlyeq c \Rightarrow c = x)$$

Definition: Smallest/Minimum
Let $\preccurlyeq$ be a partial order on the set A and $c \in A$. c is the largest element of A iff
$$\forall x \in A\ (c \preccurlyeq x)$$

Proposition: A smallest element is minimal (Lec 6)
Consider a partial order $\preccurlyeq$ on a set A. Any smallest element is minimal

Definition: Total Order Relations
If R is a partial order relation on a set A, and for any two elements x and y in A, either $x\ R\ y$ or $y\ R\ x$, then R is a total order relation (or simply total order) on A.
In other words, R is a total order iff
$$R \text{ is a partial order and } \forall x, y \in A\ x\ R\ y \vee y\ R\ x$$

Definition: Linearization of a partial order
Let $\preccurlyeq$ be a partial order on a set A. A linearization of $\preccurlyeq$ is a total order $\preccurlyeq^*$ on A such that
$$\forall x, y \in A\ x \preccurlyeq y \Rightarrow x \preccurlyeq^* y$$
(View set A as a set of tasks. $x \preccurlyeq y$ means x must be performed before y. If $x \not\preccurlyeq y$, then x and y can be performed in any order w.r.t each other)

Definition: Well-Ordered Set
Let $\preccurlyeq$ be a total order on a set A. A is well-ordered iff every non-empty subset of A contains a smallest element. Symbolically,
$$\forall S \in \mathcal{P}\ A,\ S \neq \emptyset \Rightarrow \exists x \in S\ \forall y \in S\ x \preccurlyeq y$$

Kahn's Algorithm

Input: A finite set A and a partial order $\preccurlyeq$ on A.

1. Set $A_0 \coloneqq A$ and $i \coloneqq 0$.
2. Repeat until $A_i = \emptyset$
   2.1 find a minimal element c_i of A+ wrt $\preccurlyeq$
   2.2. set $A_i + 1 = A_i \setminus \{c_i\}$
   2.3. set $i \coloneqq i + 1$

Output: A linearization $\preccurlyeq^*$ of $\preccurlyeq$ defined by setting, for all indices i, j,

$$c_i \preccurlyeq^* c_j \Leftrightarrow i \leq j$$

Theorem 8.3.1 (Equivalence Relation by Partition)
Let A be a set with a partition and let R be the relation induced by the partition. Then R is reflexive, symmetric, and transitive

Theorem 8.3.4 (Partition by Equivalence Relation)
If A is a set and R is an equivalence relation on A, then the set of distinct equivalence classes of R form a partition of A

Lemma Rel.1 (Equivalence Classes)
Let ~ be an equivalence relation on a set A. The following are equivalent for all $x, y \in A$.
(i) $x \sim y$ (ii) $[x] = [y]$ (iii) $[x] \cap [y] \neq \emptyset$

Theorem Rel.2 (Equivalence classes form partition)
Let ~ be an equivalence relation on a set A. Then $A/\sim$ is a partition of A

Congruence mod n equivalence classes

$$\{nk : k \in \mathbb{Z}\}$$
$$\{nk + 1 : k \in \mathbb{Z}\}$$
$$\ldots$$
$$\{nk + (n-1) : k \in \mathbb{Z}\}$$

Proof of Reflexivity
- suppose x ∈ Set
- utilise given relation definition to show xRx
- hence R is reflexive

Proof of Symmetry
- suppose x,y ∈ Set, s.t. xRy
- utilise given definition of relation
- show inverse also fulfils given definition
- hence yRx and R is symmetric

Proof of Transitivity
- suppose x,y,z ∈ Set, s.t. xRy and yRz
- utilise given definition of relation
- show x and z also fulfils definition
- hence xRz and R is transitive

Proof of Anti-symmetry
- suppose x,y ∈ Set, s.t. xRy and yRx
- utilise given definition of relation
- show x = y
- hence R is anti-symmetric

Proof of Partitions ($A/\sim$ is a partition of A)
- $A/\sim$ is by definition a set
- show that every element of $A/\sim$ is a nonempty subset of A
(show element is a subset of A, then show element minimally contains one member due to reflexivity)
- show every element of A is in at least one element of $A/\sim$
(utilize reflexivity)
- show every element of A is in at most one element of $A/\sim$
(assume element of A is in two elements, S_1, S_2 of $A/\sim$, then show $S_1 = S_2$)

1. ☑ In a partially ordered set, any smallest element is minimal.
2. ☑ All finite non-empty partially ordered sets have a minimal element.
3. ☑ In a partially ordered set, if there is a smallest element, there must be exactly one minimal element.
4. ☑ An infinite set partial order relation can have a smallest element. (example: consider the divisibility relation on $\mathbb{Z}^+$, 1 is the smallest element).
5. ✗ A relation that is symmetric cannot be antisymmetric.
6. ✗ A relation that is not symmetric must be antisymmetric.
7. ✗ In a partially ordered set, any minimal element is smallest.
8. ✗ There can be 2 smallest elements in some partially ordered set.
9. ✗ In a partially ordered set, if there is exactly one minimal element, then there is a smallest element. (notice that the set can be infinite with a single lone element on the side of the linear hasse diagram, which would be the minimal, as well as maximal, element).
10. ✗ If a partially ordered set does not have a smallest element, it must be an infinite set.

Misc

Definition (Even and Odd Integers)
n is even $\Leftrightarrow \exists$ an integer k such that $n = 2k$.
n is odd $\Leftrightarrow \exists$ an integer k such that $n = 2k + 1$

Definition: Divisibility
Let $n, d \in \mathbb{Z}$. Then $d \mid n \Leftrightarrow n = dk$ for some $k \in \mathbb{Z}$.

Theorem 4.3.3 (5th: 4.4.3) Transitivity of Divisibility
For all integers a, b and c, if $a \mid b$ and $b \mid c$, then $a \mid b$

Definition (Prime and Composite number)
An integer n is prime iff n > 1 and for all positive integers r and s, if n = rs, then either r or s equals n

$$n \text{ is prime} \Leftrightarrow$$
$$\forall r, s \in \mathbb{Z}^+\ n = rs \rightarrow (r = 1 \wedge s = n) \vee (r = n \wedge s = 1)$$

An integer n is composite iff n > 1 and n = rs for some integers r and s with 1 < r < n and 1 < s < n.

$$n \text{ is composite} \Leftrightarrow$$
$$\exists r, s \in \mathbb{Z}^+ \text{ s.t. } n = rs \wedge (1 < r < n) \wedge (1 < s < n)$$

Definition (Rational Numbers)
r is rational $\Leftrightarrow \exists$ integers a and b such that $r = \frac{a}{b}$ and $b \neq 0$

Theorem 4.4.1 (Quotient-Remainder Theorem)
Given any integer n and positive integer d, there exist unique integers q and r such that

$$n = dq + r \text{ and } 0 \leq r < d$$

Theorem 4.2.1 (5th: 4.3.1)
Every integer is a rational number.

Theorem 4.2.2 (5th: 4.3.2)
The sum of any two rational numbers is rational.

Corollary 4.2.3 (5th: 4.2.3)
The double of a rational number is rational.

Theorem 4.3.1 (5th: 4.4.1)
A Positive Divisor of a Positive Integer: For all positive integers a and b, if a|b, then a ≤ b.

Theorem 4.3.2 (5th: 4.4.2) Divisors of 1:
The only divisors of 1 are 1 and -1.

Theorem 4.6.1 (5th: 4.7.1)
There is no greatest integer.

Theorem 4.6.4 (5th: 4.7.4)
For all integers n, if n^2 is even then n is even

Theorem 4.7.1 (5th: 4.8.1)
$\sqrt{2}$ is irrational.

Proof (Tutorial 1 Q10)
The product of any two odd integers is an odd integer

Proof (Tutorial 1 Q11)
n^2 is odd if and only if n is odd.

Proof (Tutorial 2 Q4(a))
Integers are not closed under division.

Proof (Tutorial 2 Q4(b))
Rational numbers are closed under addition.

Proof (Tutorial 2 Q4(c))
Rational numbers are not closed under division.

Proof (Tutorial 2 Q8)
$\forall x \in \mathbb{R}((x^2 > x) \rightarrow (x < 0) \vee (x > 1))$.
↳ actually apply this

Proof (Tutorial 2 Q11)
If n is a product of two positive integers a and b, then a $\leq n^{1/2}$ or b $\leq n^{1/2}$

Proof (Tutorial 3 Q3(a))
There exist non-empty finite sets A and B such that $|A \cup B| = |A| + |B|$

Proof (Tutorial 3 Q3(b))
There exist non-empty finite sets A and B such that $|A \cup B| \neq |A| + |B|$

Proof (Tutorial 3 Q5)
$A \cap (B \setminus C) = (A \cap B) \setminus C$

Proof (Tutorial 3 Q8)
$A \subseteq B$ if and only if $A \cup B = B$

Exclusive-Or for Sets (Tutorial 3 Q7)
In A or B but not both:

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

Proof (Tutorial 4 Q2)
Let R be a relation on set A. The following are equivalent for all $x, y \in A$.

(i) symmetric, $x\,R\,y \Rightarrow y\,R\,x$
(ii) $x\,R\,y \Leftrightarrow y\,R\,x$
(iii) $R = R^{-1}$

T3 Q6.
$A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.

Proof (~~Tutorial 4 Q8(a)~~) Theorem Rel.2
If x ∈ S ∈ C, then [x] = S. (If x is an element of a component S which is an element of a partition, then the equivalence class of x is S.)

Proof (~~Tutorial 4 Q9(b)~~) Theorem Rel.2
A/~ = C (The set of equivalence classes of A is a partition of A.)

Proof (Tutorial 5 ~~Q3~~) Q5
Binary relation ⊆ on P(A) is a partial order.

Proof (Tutorial 5 ~~Q6(c)~~) Q8
For a relation R, if R is asymmetric then R is antisymmetric

Proof (Tutorial 5 ~~Q10(a)~~) 11a)
In all partially ordered sets, if two elements are comparable then they are compatible.
(In all partially ordered sets, any two comparable elements are compatible)

Properties of Integers
1. **Closure**: under addition and multiplication
2. **Commutative**: for addition and multiplication
3. **Associative**: for addition and multiplication
4. **Distributive**: Multiplication is distributive over addition but not other way round
5. **Trichotomy**: exactly one of the following is true, x = y, or x < y or x > y

***Additional Integer properties (Do not quote)**
n^2 is even if and only if n is even
Sum of two odd integers is even
Sum of two even integers is even
Sum of even and odd is odd

•) ≤ and | are partial orders w/ typical properties. Use them!
•) Well-ordered → total order → partial order
•) T5 Q8 Asymmetry → Antisymmetry

Proof Types

- By **Construction**: finding or giving a set of directions to reach the statement to be proven true. In proving equality, a useful note:

$$a \leq b \wedge a \geq b \Rightarrow a = b$$

- By **Contraposition**: proving a statement through its logically equivalent contrapositive.

- By **Contradiction**: assuming that the negation of the statement is true, which then leads to a logical contradiction.

- By **Cases**: List out the general cases and prove that statement holds in every general case

- By **Exhaustion**: considering all cases

- By **Mathematical Induction**: proving for a base case, then an induction step. In the inductive step, work from the k + 1, not the k case.
not covered yet

- By **Strong Induction**: mathematical induction assuming P (k), P (k − 1), · · · , P (a) are all true.

Proof Technique
When asked to prove 3 statements (i), (ii), (iii) are logically equivalent,
- Prove (i) ⇒ (ii)
- Prove (ii) ⇒ (iii)
- Prove (iii) ⇒ (i)

Past Midterm Notes

- When proving/disproving, don't forget about <-> = both ways
- Take note of words like **unique, different, only if, etc.**
- Absorption law is **underused**
- Don't immediately expand a logical statement: consider adding a universal statement like or $\ldots \wedge (p \vee \sim p)$
- Pay attention to definitions of sets and orders **especially with comparisons.**
- e.g. May be true for x < y but is it true for x > y?
- Try to take shortcuts through stuff learnt in tutorials.
- Introduce universal/existential statments only when required. Try to not dump variables all at the start.
- Order of variables in universeal/existential statements **matter**. Best way is to try to interpret them in English.
- Always **double** check for **transitivity**! Not all elements need reflexivity in transitivity.
- Argument is **unsound** = premises are not all true. ==> argument is vacuously valid
- Only **invalid** if premises are all true but conclusion is not true.

Any relation on $\emptyset$:
•) Reflexive
•) Irreflexive
•) Transitive
•) Symmetric
•) Antitransitive
•) Antisymmetric
•) Asymmetric

A relation $R = \{\}$ on a non-empty A:
•) Not reflexive
•) Irreflexive
•) Symmetric
•) Antisymmetric
•) Asymmetric
•) Transitive
•) Anti-transitive

Asymmetry
$\Leftrightarrow$
Irreflexive and Antisymmetry

Any element in R where R is transitive or symmetric; xRx
‼ but not the elements not R-related to anything

Don't forget of xRx only in posets!
They are both maximal & minimal
& any part ord is REFLEXIVE

Break down absolutes in universal or existential statements.
↳ takes shorter than you'd expect.

•) $P(A \cap B) = P(A) \cap P(B)$
but $P(A \cup B) \neq P(A) \cup P(B)$

•) Well-ordered set:
all non-$\emptyset$ subsets have smallest els;
including infinite subsets.

•) Generally, no other relations between refl, asymm, antisym, symm, trans, or antitrans.
↳ most $\Leftrightarrow$ can be broken by counter e.g.

•) R reflexive $\wedge$ S symmetric
$\therefore R \cup S$ is reflexive.
★ always consider how 2 relations involve entirely different elements.

•) $R \circ R = R$
$R = R^{-1}$
$R \circ R^{-1} = R^{-1} \circ R$
and any other corresponding formula
} for R is an eqv reltn

•) Binary relation $\subseteq$ on $\mathbb{R}$ is a partial order.
(Tutorial 5 Qn. 5)

•) $(p \to q) \wedge (q \to r)$
$\cdot\, p \to r$
} valid

but $(p \to q) \to r \not\equiv p \to (q \to r)$ by T1Q4

The real numbers also satisfy the following axioms, called the **order axioms.** It is assumed that among all real numbers there are certain ones, called the **positive real numbers**, that satisfy properties Ord1, Ord2, and Ord3.

Ord1. For any real numbers a and b, if a and b are positive, so are $a+b$ and ab.

Ord2. For every real number $a \neq 0$, either a is positive or $-a$ is positive but not both.

Ord3. The number 0 is not positive.

The symbols $<$, $>$, $\leq$, and $\geq$, and negative numbers are defined in terms of positive numbers.

Definition

Given real numbers a and b,

$a < b$ means $b + (-a)$ is positive. $\quad$ $b > a$ means $a < b$.
$a \leq b$ means $a < b$ or $a = b$. $\quad$ $b \geq a$ means $a \leq b$.
If $a < 0$, we say that a is **negative.** $\quad$ If $a \geq 0$, we say that a is **nonnegative.**

From the order axioms Ord1, Ord2, and Ord3 and the above definition, all the usual rules for calculating with inequalities can be derived. The most important are collected as theorems T17, T18, T19, T20, T21, T22, T23, T24, T25, T26, and T27 as follows. In all these theorems the symbols $a, b, c,$ and d represent arbitrary real numbers.

T17. *Trichotomy Law* For arbitrary real numbers a and b, exactly one of the three relations $a < b$, $b < a$, or $a = b$ holds.

T18. *Transitive Law* If $a < b$ and $b < c$, then $a < c$.

T19. If $a < b$, then $a + c < b + c$.

T20. If $a < b$ and $c > 0$, then $ac < bc$.

T21. If $a \neq 0$, then $a^2 > 0$.

T22. $1 > 0$.

T23. If $a < b$ and $c < 0$, then $ac > bc$.

T24. If $a < b$, then $-a > -b$. In particular, if $a < 0$, then $-a > 0$.

T25. If $ab > 0$, then both a and b are positive or both are negative.

T26. If $a < c$ and $b < d$, then $a + b < c + d$.

T27. If $0 < a < c$ and $0 < b < d$, then $0 < ab < cd$.

F1. *Commutative Laws* For all real numbers a and b,

$$a+b=b+a \quad \text{and} \quad ab=ba.$$

F2. *Associative Laws* For all real numbers a, b, and c,

$$(a+b)+c=a+(b+c) \quad \text{and} \quad (ab)c=a(bc).$$

F3. *Distributive Laws* For all real numbers a, b, and c,

$$a(b+c)=ab+ac \quad \text{and} \quad (b+c)a=ba+ca.$$

F4. *Existence of Identity Elements* There exist two distinct real numbers, denoted 0 and 1, such that for every real number a,

$$0+a=a+0=a \quad \text{and} \quad 1\cdot a=a\cdot 1=a.$$

F5. *Existence of Additive Inverses* For every real number a, there is a real number, denoted $-a$ and called the **additive inverse** of a, such that

$$a+(-a)=(-a)+a=0.$$

F6. *Existence of Reciprocals* For every real number $a \neq 0$, there is a real number, denoted $1/a$ or a^{-1}, called the **reciprocal** of a, such that

$$a\cdot\left(\frac{1}{a}\right)=\left(\frac{1}{a}\right)\cdot a=1.$$

T1. *Cancellation Law for Addition* If $a+b=a+c$, then $b=c$. (In particular, this shows that the number 0 of Axiom F4 is unique.)

T2. *Possibility of Subtraction* Given a and b, there is exactly one x such that $a+x=b$. This x is denoted by $b-a$. In particular, $0-a$ is the additive inverse of a, $-a$.

T3. $b-a=b+(-a)$.

T4. $-(-a)=a$.

T5. $a(b-c)=ab-ac$.

T6. $0\cdot a=a\cdot 0=0$.

T7. *Cancellation Law for Multiplication* If $ab=ac$ and $a\neq 0$, then $b=c$. (In particular, this shows that the number 1 of Axiom F4 is unique.)

T8. *Possibility of Division* Given a and b with $a\neq 0$, there is exactly one x such that $ax=b$. This x is denoted by b/a and is called the **quotient** of b and a. In particular, $1/a$ is the reciprocal of a.

T9. If $a\neq 0$, then $b/a=b\cdot a^{-1}$.

T10. If $a\neq 0$, then $\left(a^{-1}\right)^{-1}=a$.

T11. *Zero Product Property* If $ab=0$, then $a=0$ or $b=0$.

T12. *Rule for Multiplication with Negative Signs*

$$(-a)b=a(-b)=-(ab), \quad (-a)(-b)=ab,$$

and

$$-\frac{a}{b}=\frac{-a}{b}=\frac{a}{-b}.$$

T13. *Equivalent Fractions Property*

$$\frac{a}{b}=\frac{ac}{bc}, \quad \text{if } b\neq 0 \text{ and } c\neq 0.$$

T14. *Rule for Addition of Fractions*

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}, \quad \text{if } b\neq 0 \text{ and } d\neq 0.$$

T15. *Rule for Multiplication of Fractions*

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}, \quad \text{if } b\neq 0 \text{ and } d\neq 0.$$

T16. *Rule for Division of Fractions*

$$\frac{\frac{a}{b}}{\frac{c}{d}}=\frac{ad}{bc}, \quad \text{if } b\neq 0,\, c\neq 0, \text{ and } d\neq 0.$$