CS1231S Summary Sheet

Important Sets

$\mathbb{N}$:	Set of all natural numbers (includes 0)
$\mathbb{Z}$:	Set of all integers
$\mathbb{Q}$:	Set of all rational numbers
$\mathbb{R}$:	Set of all real numbers
$\mathbb{Z}_{\geq 0}$:	Set of all non-negative integers

Basic Properties of Integers

Closure:	Integers are closed under addition and multiplication
Commutativity:	Addition and multiplication are commutative
Associativity:	Addition and multiplication are associative
Distributivity:	Multiplication is distributed over addition (but not other way round)
Trichotomy:	Exactly one of the following is true: *x = y, or x < y, or x > y.*

Definition: Even and Odd Integers

$n \text{ is even} \leftrightarrow \exists k \in \mathbb{Z} \text{ such that } n = 2k$

$n \text{ is odd} \leftrightarrow \exists k \in \mathbb{Z} \text{ such that } n = 2k + 1$

Definition: Divisiblity

$d|n \leftrightarrow \exists k \in \mathbb{Z} \text{ such that } n = dk$

Theorem 4.7.1 Irrationality of $\sqrt{2}$

$\sqrt{2}$ is irrational.

Definition: Rational and irrational numbers

A real number r is **rational** iff it can be expressed as a quotient of two integers with a nonzero denominator.

$$r \text{ is rational} \leftrightarrow \exists a, b \in \mathbb{Z}\ s.t.\ r = \frac{a}{b} \text{ and } b \neq 0$$

A real number that is not rational is **irrational**.

Order of operations:

$\sim$ (not), $\wedge / \vee$ (and/or), $\rightarrow \leftrightarrow$ (if-then, iff)

Definition: Fraction in lowest term

A quotient of two integers with a a nonzero denominator is also commonly known as a fraction. A fraction $\frac{a}{b}$ $(where\ b \neq 0)$ is said to be in lowest terms if the largest integer that divides both a and b is 1.

Definitions: Prime and Composite

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.

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

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

N is composite: $\exists r, s \in \mathbb{Z}^+,$
$(n = rs \wedge (1 < r < n) \wedge (1 < s < n))$

Theorem 4.2.1:	Every integer is a rational number.
Theorem 4.2.2:	The sum of any two rational numbers is rational.
Corollary 4.2.3:	The double of a rational number is rational.
Theorem 4.3.1:	For all positive integers a and b, $if\ a|b, then\ a \leq b$.
Theorem 4.3.2 :	The only divisors of 1 are 1 and -1.
Theorem 4.3.3:	For all integers a, b, and c, if $a|b$ and $b|c$, then $a|c$.
Proposition 4.6.4:	For all integer n, if n^2 is even, then n is even.
Theorem 4.6.1	`There is no greatest integer.

Definition 2.1.1 (Statement)

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

Definition 2.1.5 (Statement Form/Propositional Form)

A statement form (or proposition 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 2.2.1 (Conditional)

If p and q are statement variables, the condition of q by p is
"if p then q" denoted $p \rightarrow q$.
It is false when p is true and q is false; otherwise it is true.
We call p the hypothesis/antecedent and q the conclusion/consequence.

Definition 2.2.2 (Contrapositive): **The contrapositive of $p \rightarrow q$ is $\sim q \rightarrow \sim p$.**
Definition 2.2.3 (Converse): **The converse of $p \rightarrow q$ is $q \rightarrow p$.**
Definition 2.2.4 (Inverse): **The inverse of $p \rightarrow q$ is $\sim p \rightarrow \sim q$.**
Implication Law: $p \rightarrow q \equiv \sim p \vee q$

Definition 2.2.5 (Only If)

"p only if q" means **"if not q then not p"** or **"$\sim q \rightarrow \sim p$".**
Or equivalently, **"if p then q"** or **"$p \rightarrow q$"**

Definition 2.2.6 (Biconditional)

Given statement variables p and q, the biconditional of p and q is
"p if, and only if, q" denote $p \leftrightarrow q$.
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 and Sufficient Conditions)

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

Definition 2.3.1 (Argument)

An argument (argument form) is a sequence of statements (statement forms). All statements except for the final one are called premises. The final statement is called the conclusion. An argument is valid if no matter what particular statements are substituted for the statement variables in the premises, if the resulting premises are all true, the conclusion is also true.

Definition 2.3.2 (Sound and Unsound argument)

An argument is sound iff it is valid and all its premises are true. An argument that is not sound is called unsound.

Theorem 2.1.1 Logical Equivalences

Commutative Laws	$p \wedge q \equiv q \wedge p$ $p \vee q \equiv q \vee p$
Associative Laws	$p \wedge q \wedge r \equiv (p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ $p \vee q \vee r \equiv (p \vee q) \vee r \equiv p \vee (q \vee r)$
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	$p \wedge true = p$ $p \vee false \equiv p$
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	$\sim(p \wedge q) \equiv \sim p \vee \sim q$
Absorption Laws	$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$
Negation of true/false	$\sim true = false$ $\sim false = true$

Table 2.3.1 Rules of Inference

Modus Ponens	$p \to q$ p $\therefore q$	**Elimination**	$p \vee q$ $p \vee q$ $\sim q$ $\sim p$ $\therefore p$ $\therefore q$
Modus Tollens	$p \to q$ $\sim q$ $\therefore \sim p$	**Transitivity**	$p \to q$ $q \to r$ $\therefore p \to r$
Generalization	p q $\therefore p \vee q$ $\therefore p \vee q$	**Proof by Division Into Cases**	$p \vee q$ $p \to r$ $q \to r$ $\therefore r$
Specialization	$p \wedge q$ $p \wedge q$ $\therefore p$ $\therefore q$	**Contradiction Rule**	$\sim p \to false$ p
Conjunction	p q $\therefore p \wedge q$		

Fallacies: Converse Error

$p \to q$

q

$\therefore p$

Fallacies: Inverse Error

$p \to q$

$\sim p$

$\therefore \sim q$

Definition 3.1.1: Predicate

A **predicate** is a sentence that contains a finite number of variables and becomes a statement when specific variables are substituted for the variables. The **domain** of a predicate variable is the set of all variables that may be substituted in place of the variable.

- Domain may also be known as domain of discourse, universe of discourse, universal set, or simply universe.

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 makes P(X) true when they are substituted for x.
The truth set of P(X) is denoted $\{x \in D \mid P(x)\}$.

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 atleast 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 $\exists x \in D \text{ such that } Q(x)$.

- It is defined to be true iff Q(x) is true for atleast 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 a Universal Statement

$$\sim\left(\forall x \in D, P(x)\right) \equiv \exists x \in D \text{ such that } \sim P(x)$$

Theorem 3.2.2: Negation of an Existential Statement

$$\sim\left(\exists x \in D \text{ such that } P(x)\right) \equiv \forall x \in D, \sim P(x)$$

Universal Quantified Statement

$\forall x \in D(P(x) \to Q(x))$ is called vacuously true or true by default iff P(x) is false for every x in D.

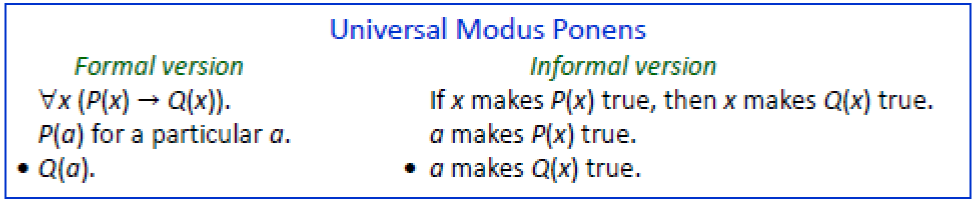
Definition 3.2.1 (Contrapositive, converse, inverse)

Consider a statement of the form: $\forall x \in D(P(x) \to Q(x))$

1. Its **contrapositive** is: $\forall x \in D(\sim Q(x) \to \sim P(x))$
2. Its **converse** is $\forall x \in D(Q(x) \to P(x))$
3. Its **inverse** is $\forall x \in D(\sim P(x) \to \sim Q(x))$

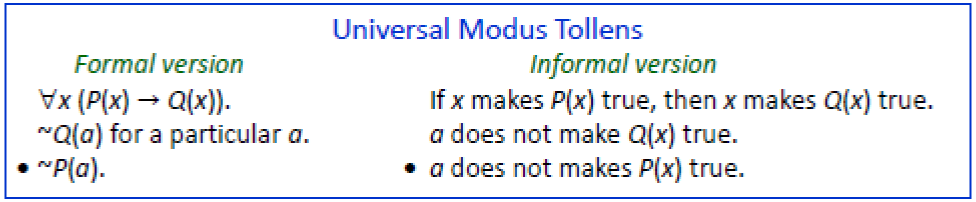
Definition 3.2.2: Necessary and Sufficient conditions, Only if

- $\forall x, r(x)$ is a sufficient condition for s(x) means $\forall x(r(x) \rightarrow s(x))$
- $\forall x, r(x)$ is a necessary condtion for s(x) means $\forall x(\sim r(x) \rightarrow \sim s(x))$ or equivalently, $\forall x(s(x) \rightarrow r(x))$
- $\forall x, r(x)$ only if s(x) means $\forall x\big(\sim s(x) \rightarrow \sim r(x)\big)$ or equivalently, $\forall x(r(x) \rightarrow s(x))$



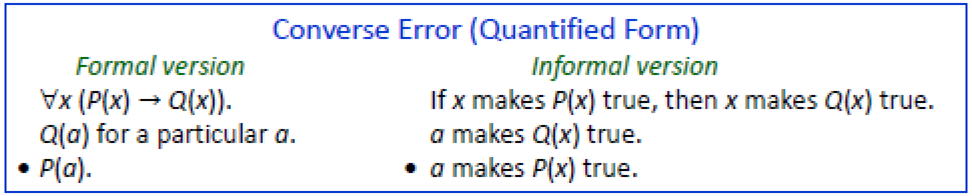
Universal Modus Ponens

Formal version	*Informal version*
∀x (*P*(*x*) → *Q*(*x*)).	If *x* makes *P*(*x*) true, then *x* makes *Q*(*x*) true.
P(*a*) for a particular *a*.	*a* makes *P*(*x*) true.
• *Q*(*a*).	• *a* makes *Q*(*x*) true.



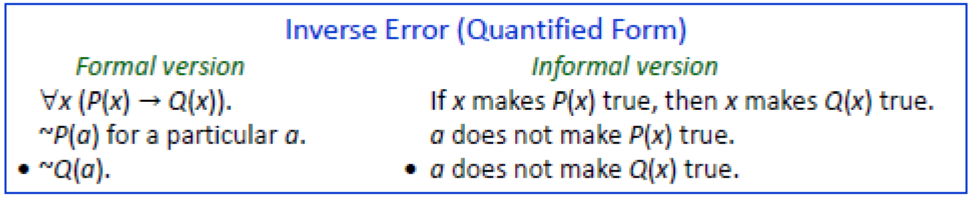
Universal Modus Tollens

Formal version	*Informal version*
∀x (*P*(*x*) → *Q*(*x*)).	If *x* makes *P*(*x*) true, then *x* makes *Q*(*x*) true.
~*Q*(*a*) for a particular *a*.	*a* does not make *Q*(*x*) true.
• ~*P*(*a*).	• *a* does not makes *P*(*x*) true.



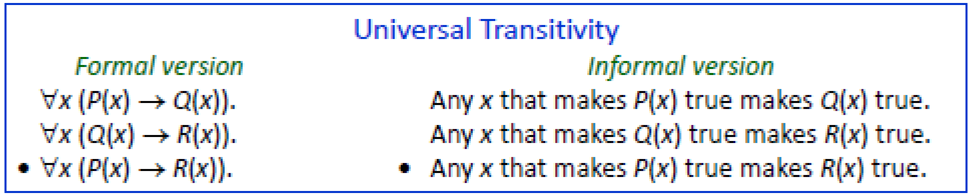
Converse Error (Quantified Form)

Formal version	*Informal version*
∀x (*P*(*x*) → *Q*(*x*)).	If *x* makes *P*(*x*) true, then *x* makes *Q*(*x*) true.
Q(*a*) for a particular *a*.	*a* makes *Q*(*x*) true.
• *P*(*a*).	• *a* makes *P*(*x*) true.



Inverse Error (Quantified Form)

Formal version	*Informal version*
∀x (*P*(*x*) → *Q*(*x*)).	If *x* makes *P*(*x*) true, then *x* makes *Q*(*x*) true.
~*P*(*a*) for a particular *a*.	*a* does not make *P*(*x*) true.
• ~*Q*(*a*).	• *a* does not make *Q*(*x*) true.



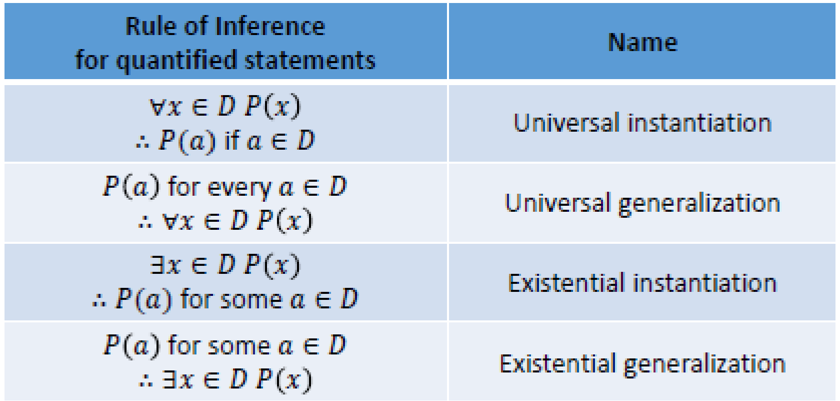
Universal Transitivity

Formal version	*Informal version*
∀x (*P*(*x*) → *Q*(*x*)).	Any *x* that makes *P*(*x*) true makes *Q*(*x*) true.
∀x (*Q*(*x*) → *R*(*x*)).	Any *x* that makes *Q*(*x*) true makes *R*(*x*) true.
• ∀x (*P*(*x*) → *R*(*x*)).	• Any *x* that makes *P*(*x*) true makes *R*(*x*) true.

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 symbol in its premises, if the resulting premise statements are all true, then the conclusion is also true.

An argument is called valid iff its form is valid.



Rule of Inference for quantified statements	Name
$\forall x \in D\ P(x)$ $\therefore P(a)$ if $a \in D$	Universal instantiation
$P(a)$ for every $a \in D$ $\therefore \forall x \in D\ P(x)$	Universal generalization
$\exists x \in D\ P(x)$ $\therefore P(a)$ for some $a \in D$	Existential instantiation
$P(a)$ for some $a \in D$ $\therefore \exists x \in D\ P(x)$	Existential generalization

Set-Roster Notation

A set may be specified by writing all of its elements between braces.

Examples: {1, 2, 3}, {1, 2, 3, …, 100}

The symbol … is called an ellipsis and is read "and so forth"

- Order and duplicates DO NOT matter

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.

Set-Builder Notation

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

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

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 ranges over the elements of A is denoted

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

To check whether an object z is an element of $S = \{t(x): x \in A\}$: If there is an $x \in A$ such that t(x) = z, then $z \in S$, else $z \notin S$.

Definition: Subset

Let A and B be sets. A is a subset of B, written $A \subseteq B$, iff every element of A is also an element of B.

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

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.

Set A not a subset of Set B

$A \nsubseteq B \leftrightarrow \exists x(x \in A \wedge x \notin B)$

Theorem 6.2.4

An empty set is a subset of every set, i.e. $\emptyset \subseteq A$ for all sets A.

- A set with no element, { }, is an empty set, denoted as $\emptyset$.

Singleton

A set with exactly one element is called a **singleton**.

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.

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

Definition: Cartesian Product

Given sets A and B, the Cartesian product of A and B, denoted $A \times B$ and read "A cross B", is the set of all ordered pairs (a,b) where a is in A and b is in B.

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

Definition: Set Equality

Given sets A and B, A equals B, written A = B iff every element of A is in B and every element of B is in A.

$$A = B \leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$$

or $A = B \leftrightarrow \forall x(x \in A \leftrightarrow x \in B)$

Basic method for proving that two sets are equals:

1. Let sets X and Y be given. To prove X = Y
2. $(\subseteq)\ Prove\ that\ X \subseteq Y$
3. $(\supseteq)\ Prove\ that\ Y \subseteq X\ (or\ X \supseteq Y)$
4. From (2) and (3), conclude that X = Y

Definitions (Union, Intersection, Difference, Complement)

Let A and B be subsets of a universal set U.

1. The **union** of A and B, denoted $A \cup B$, is the set of all elements that are in atleast one of A or B
2. The **intersection** of A and B, denoted $A \cap B$, is the set of all elements that are common to both A and B.
3. The **difference** of B minus A (or relative complement of A in B), denoted **B – A**, or **B\A**, is the set of all elements that are in B and not A.
4. The complement of A, denoted $\bar{A}$, is the set of all elements in U that are not in A.

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

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

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

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

Notation

Given real numbers a and b, with $a \le b$:

$(a, b) = \{x \in \mathbb{R} : a < x < b\}$ $[a, b] = \{x \in \mathbb{R} : a \le x \le b\}$

$(a, b] = \{x \in \mathbb{R} : a < x \le b\}$ $[a, b) = \{x \in \mathbb{R} : a \le x < b\}$

The symbol ∞ and $-\infty$ are used to indicated intervals that are unbounded either on the right or on the left:

$(a, \infty) = \{x \in \mathbb{R} : x > a\}$ $[a, \infty) = \{x \in \mathbb{R} : x \ge a\}$

$(-\infty, b) = \{x \in \mathbb{R} : x < b\}$ $(-\infty, b] = \{x \in \mathbb{R} : x \le b\}$

Definition: Disjoint

Two sets are **disjoint** iff they have no elements in common.

$$A \text{ and } B \text{ are disjoint } iff\ A \cap B = \emptyset$$

Definition: Mutually Disjoint

Sets $A_1, A_2, A_3, \ldots$ are mutually disjoint iff no two sets A_i and A_j with distinct subscripts have any elements in common.

$$A_i \cap B_j = \emptyset \text{ whenever } i \ne j$$

Definition: Unions and Intersections of an Indexed Collection of Sets

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

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

$$\bigcup_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \ \ for\ atleast\ one\ nonnegative\ integer\ i\}$$

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

$$\bigcap_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \ \ for\ all\ nonnegative\ integer\ i\}$$

Theorem 4.4.1: Quotient-Remainder Theorem

Given any integer n and positive integer d, there exists unique integers q and r such that

$$n = dq + r \ \ and \ \ 0 \le r < d$$

Definition: Power Set

Given a set A, the **power set** of A, denoted $\wp(A)$, is the set of all subsets of A

- $Let\ A = \{x, y\}$

$$\wp(A) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$$

Theorem 6.3.1: Cardinality of power set

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

Definition: Ordered n-tuples

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

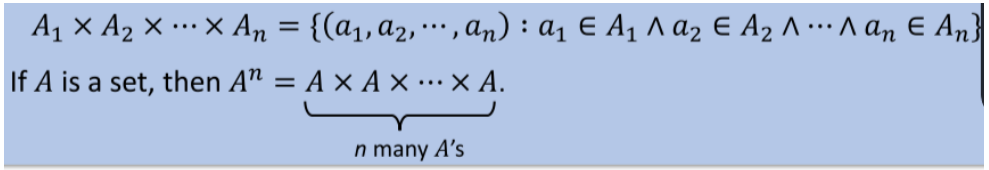
An ordered pair is an ordered 2-tuple, and ordered triple is an ordered 3-tuple.

Equality of two ordered n-tuples:

$$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \leftrightarrow x_1 = y_1, x_2 = y_2, \ldots, x_n = y_n$$

Definition: Cartesian Product

Given sets A_1, A_2,$\cdots$, A_n, the Cartesian product of A_1, A_2,$\cdots$, A_n, denoted $A_1 \times A_2 \times \cdots \times A_n$, is the set of all ordered n-tuples (a_1, a_2,$\cdots$, a_n) where $a_1 \in A_1$, $a_2 \in A_2$,$\cdots$, $a_n \in A_n$.



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

If A is a set, then $A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ many } A\text{'s}}$.

Theorem 6.2.1: Some Subset Relations

1. **Inclusion of Intersection:** For all sets A and B,
   a. $A \cap B \subseteq A$ b. $A \cap B \subseteq B$
2. **Inclusion in Union:** For all sets A and B,
   a. $A \subseteq A \cup B$ b. $B \subseteq A \cup B$
3. **Transitive Property of Subsets:** For all sets A,B, and C,
   $A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$

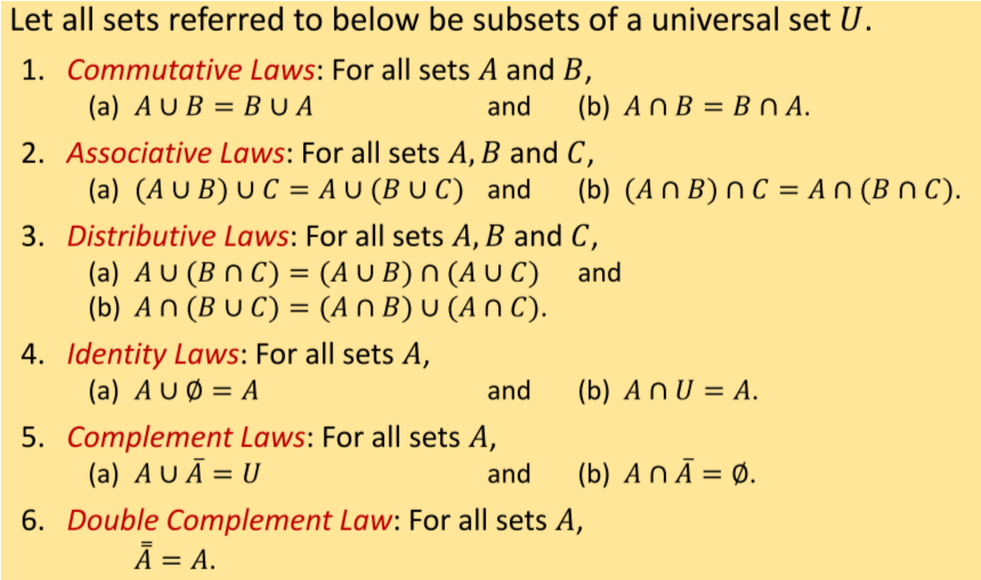
Procedural Versions of Set Definitions

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. $(a, b) \in X \times Y \leftrightarrow a \in X \wedge b \in Y$

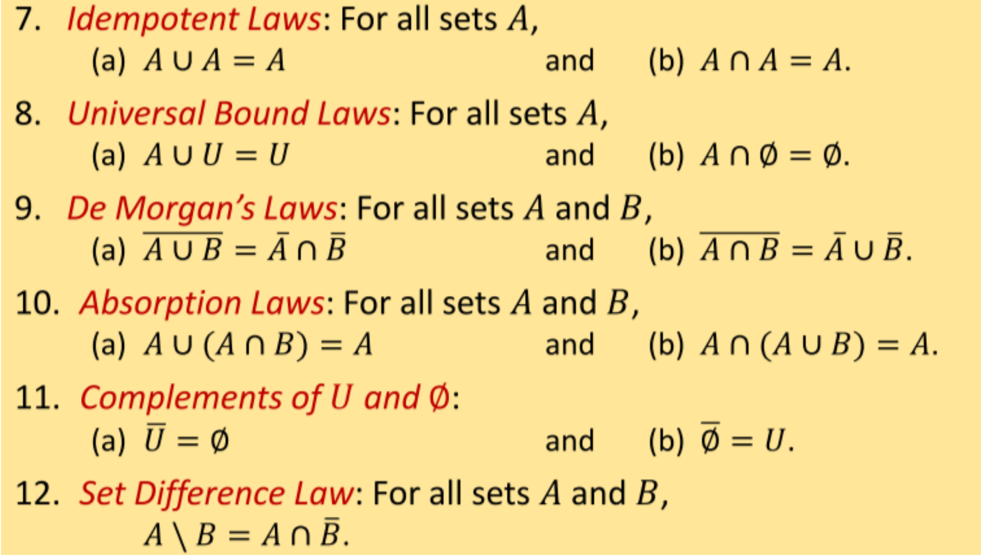
Note: In a context where U is the universal set, the complement of X is defined by $\bar{X} = U \setminus X$.

Theorem 6.2.2 Set Identities



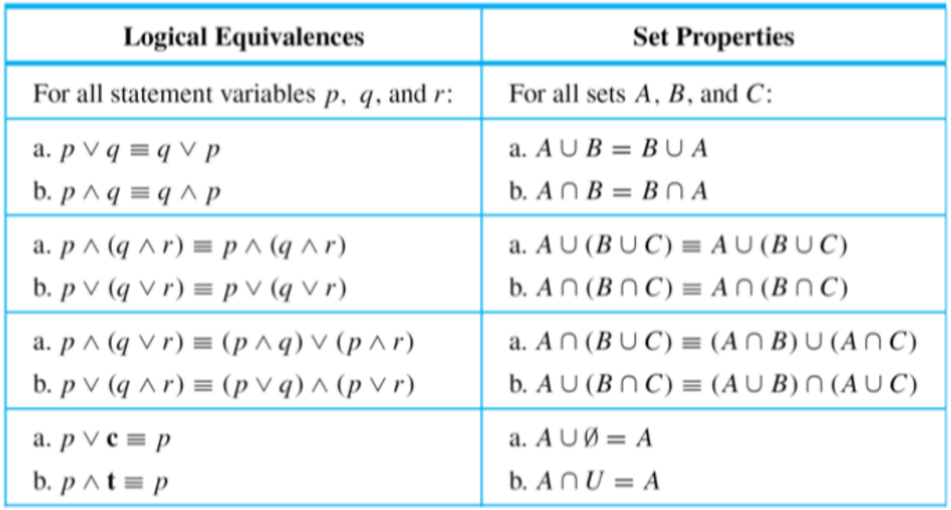
Let all sets referred to below be subsets of a universal set U.

1. *Commutative Laws*: For all sets A and B,
   (a) $A \cup B = B \cup A$ and (b) $A \cap B = B \cap A$.
2. *Associative Laws*: For all sets A, B and C,
   (a) $(A \cup B) \cup C = A \cup (B \cup C)$ and (b) $(A \cap B) \cap C = A \cap (B \cap C)$.
3. *Distributive Laws*: For all sets A, B and C,
   (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and
   (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
4. *Identity Laws*: For all sets A,
   (a) $A \cup \emptyset = A$ and (b) $A \cap U = A$.
5. *Complement Laws*: For all sets A,
   (a) $A \cup \bar{A} = U$ and (b) $A \cap \bar{A} = \emptyset$.
6. *Double Complement Law*: For all sets A,
   $\bar{\bar{A}} = A$.

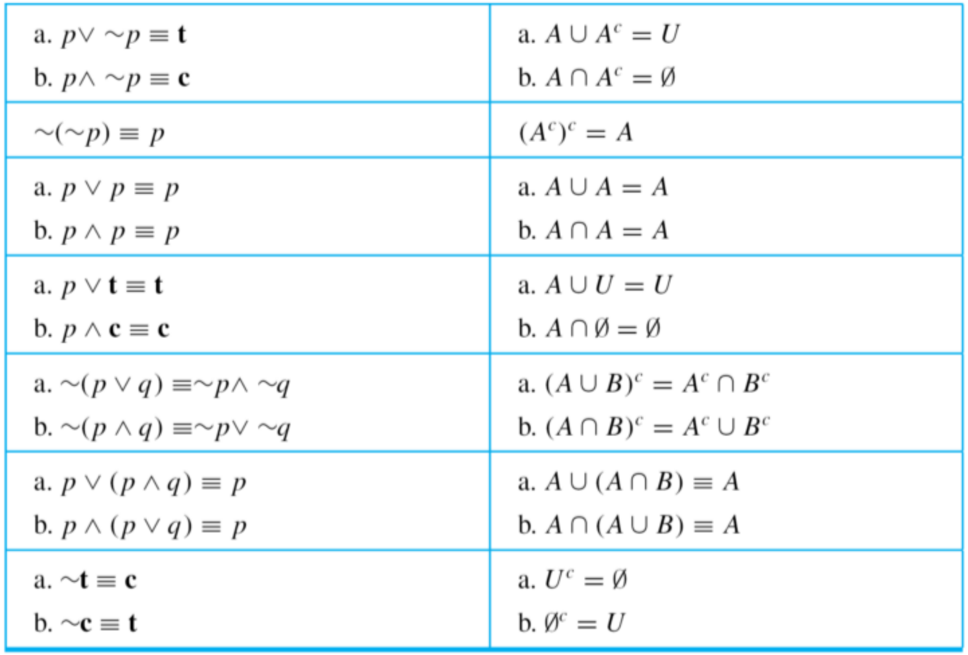


7. *Idempotent Laws*: For all sets A,
   (a) $A \cup A = A$ and (b) $A \cap A = A$.
8. *Universal Bound Laws*: For all sets A,
   (a) $A \cup U = U$ and (b) $A \cap \emptyset = \emptyset$.
9. *De Morgan's Laws*: For all sets A and B,
   (a) $\overline{A \cup B} = \bar{A} \cap \bar{B}$ and (b) $\overline{A \cap B} = \bar{A} \cup \bar{B}$.
10. *Absorption Laws*: For all sets A and B,
    (a) $A \cup (A \cap B) = A$ and (b) $A \cap (A \cup B) = A$.
11. *Complements of U and $\emptyset$*:
    (a) $\bar{U} = \emptyset$ and (b) $\bar{\emptyset} = U$.
12. *Set Difference Law*: For all sets A and B,
    $A \setminus B = A \cap \bar{B}$.

Table 6.4.1 Logical Equivalence



Logical Equivalences	Set Properties
For all statement variables p, q, and r:	For all sets A, B, and C:
a. $p \vee q \equiv q \vee p$ b. $p \wedge q \equiv q \wedge p$	a. $A \cup B = B \cup A$ b. $A \cap B = B \cap A$
a. $p \wedge (q \wedge r) \equiv p \wedge (q \wedge r)$ b. $p \vee (q \vee r) \equiv p \vee (q \vee r)$	a. $A \cup (B \cup C) \equiv A \cup (B \cup C)$ b. $A \cap (B \cap C) \equiv A \cap (B \cap C)$
a. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ b. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	a. $A \cap (B \cup C) \equiv (A \cap B) \cup (A \cap C)$ b. $A \cup (B \cap C) \equiv (A \cup B) \cap (A \cup C)$
a. $p \vee \mathbf{c} \equiv p$ b. $p \wedge \mathbf{t} \equiv p$	a. $A \cup \emptyset = A$ b. $A \cap U = A$



a. $p \vee \sim p \equiv \mathbf{t}$ b. $p \wedge \sim p \equiv \mathbf{c}$	a. $A \cup A^c = U$ b. $A \cap A^c = \emptyset$
$\sim(\sim p) \equiv p$	$(A^c)^c = A$
a. $p \vee p \equiv p$ b. $p \wedge p \equiv p$	a. $A \cup A = A$ b. $A \cap A = A$
a. $p \vee \mathbf{t} \equiv \mathbf{t}$ b. $p \wedge \mathbf{c} \equiv \mathbf{c}$	a. $A \cup U = U$ b. $A \cap \emptyset = \emptyset$
a. $\sim(p \vee q) \equiv \sim p \wedge \sim q$ b. $\sim(p \wedge q) \equiv \sim p \vee \sim q$	a. $(A \cup B)^c = A^c \cap B^c$ b. $(A \cap B)^c = A^c \cup B^c$
a. $p \vee (p \wedge q) \equiv p$ b. $p \wedge (p \vee q) \equiv p$	a. $A \cup (A \cap B) \equiv A$ b. $A \cap (A \cup B) \equiv A$
a. $\sim\mathbf{t} \equiv \mathbf{c}$ b. $\sim\mathbf{c} \equiv \mathbf{t}$	a. $U^c = \emptyset$ b. $\emptyset^c = U$

Methods of Proofs

Constructive Proof

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

To prove such statement, we may use **constructive proofs of existence:**

- Find an x in D that makes Q(x) true
- Give a set of directions for finding such an x

Disproof by Counterexample

$$\forall x \in D\ (P(x) \rightarrow Q(x))$$

To disprove such statement, we can find a **counterexample**.

- Find a value of x in D for which hypothesis P(x) is true, but conclusion Q(x) is false.

Method of exhaustion

$$\forall x \in D\ (P(x) \rightarrow Q(x))$$

When D is finite or when only a finite number of elements satisfy P(x), we may prove the statement by the **method of exhaustion.**

Generalizing from the Generic Particular

To show that every element of a set satifies a certain property, suppose x is a particular but arbitrarily chosen element of the set, and show that x satisfies the property.

Indirect Proof: Proof by contradiction

1. Suppose the statement to be proved, S, is false. That is the negation of the statement ~S is true.
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement S is true.

Indirect Proof: Proof by contraposition

1. Statement to be proved: $\forall x \in D\ (P(x) \rightarrow Q(x))$
2. Rewrite the statement into its contrapositive form:

$$\forall x \in D\ (\sim Q(x) \rightarrow \sim P(x))$$

3. Prove the contrapositive statement by a direct proof.
    3.1 Suppose x is some element of D s.t. Q(x) is false
    3.2 Show that P(x) is false
4. Therefore the original statement … is true.

Definition: Relation

Let A and B be sets. 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**, or x is R-related to y, written $x\ R\ y$, **iff** $(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{R}$.

- $x\ R\ y\ means\ (x, y) \in R$
  $x \not R\ y$ means $(x, y) \notin$ R

Definition: 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), is the set $\{a \in A : aRb\ for\ some\ b \in B\}$.
The co-domain of R, coDom(R), is the set B.
The range of R, Range(R), is the set $\{b \in B : aRb\ for\ some\ a \in A\}$.

Example: Let A=$\{1,2,3\}$and B=$\{2,4,9\}$, and define a relation R from A to B as follows: $\forall x,y \in A \times B,\ x,y \in R \Leftrightarrow x^2 = y$.
$Dom(R)$ $= \{2,3\}$
$coDom(R)$ $= \{2,4,9\}$
$Range(R)$ $= \{4,9\}$

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:

$$R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\}$$
$$\forall x \in A, \forall y \in B\ ((y, x) \in R^{-1} \leftrightarrow (x, y) \in R)$$

Note: R and R^{-1} has the same properties (reflexive, transitive, etc)

Definition: Relation on a Set

A relation on a set 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: 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:

$$\forall x \in A, \forall z \in C(xS \circ Rz \leftrightarrow (\exists y \in B\ (xRy \wedge ySz)))$$

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.

$$T \circ (S \circ R) = (T \circ S) \circ R = T \circ S \circ R$$

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.

$$(S \circ R)^{-1} = R^{-1} \circ S^{-1}$$

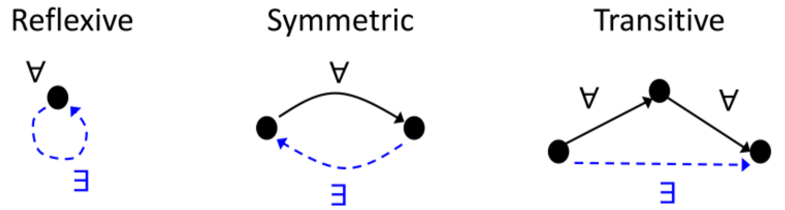
Definition: n-ary Relation

Given n sets $A_1, A_2, \ldots, A_n$, an n-ary relation R on $A_1 \times A_2 \times \ldots \times A_n$ is a subset of $A_1 \times A_2 \times \ldots \times A_n$.
The special cases of 2-ary, 3-ary… are called binary, ternary, and quaternary relations respectively.

Definitions: Reflectivity, Symmmetry, Transitivity

Let R be a relation on a set A.

1. R is reflective iff $\forall x \in A\ (xRx)$
2. R is symmetric iff $\forall x, y \in A\ (xRy \rightarrow yRx)$
3. R is transitive iff $\forall x, y, z \in A\ (xRy \wedge yRz \rightarrow xRz)$


Reflexive
Symmetric
Transitive

Note: Reflexivity, symmetry, and transitivity are properties of a relation, not properties of members of the set.

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

The relation obtained by adding the least number of ordered pairs to ensure transitivity is called the transitive closure of the relation.

Definition: Partition

A partition of set A is a finite or infinite collection of nonempty, mutually disjoint subsets whose union is A.

$\mathcal{C}$ is a partition of set A if the following hold:

1. $\mathcal{C}$ is a set of which all elements are non-empty subsets of A, i.e
   $\emptyset \neq S \subseteq A \ \ for\ all\ S \in \mathcal{C}$
2. Every element of A is in exactly one element of $\mathcal{C}$, i.e.,
   $\forall x \in A\ \exists S \in \mathcal{C}\ (\mathrm{x} \in \mathrm{S})\ and$
   $\forall x \in A\ \exists S_1, S_2 \in \mathcal{C}\ (\mathrm{x} \in \mathrm{S}_1 \wedge x \in S_2 \rightarrow S_1 = S_2)$

Elements of a partition are called components of the partition.

A partition of set A is a set $\mathcal{C}$ of non-empty subsets of A such that

$$\forall x \in A\ \exists!\, S \in \mathcal{C}\ (x \in S)$$

Definition: Relation Induced by a Partition

Given a partition $\mathcal{C}$ of a set A, the **relation R induced by the partition** is defined on A as follows: $\forall x, y \in A$,

$$xRy \leftrightarrow \exists\ a\ component\ S\ of\ \mathcal{C}\ \mathrm{s.t.}\ \ \mathrm{x, y \in S}$$

Theorem 8.3.1 Relation induced by a 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**.

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**.

Note: The symbol ~ is commonly used to denote an equivalence relation.

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 [a] and called the **class of a** for short, is the set of all elements $x \in A$ s.t. a is ~- related to x

$$[a]_\sim = \{x \in A : a \sim x\}$$
$$\forall x \in A (x \in [a]_\sim \leftrightarrow a \sim x)$$

Lemma Rel.1 Equivalence Classes

Let ~ be an equivalence relation on a set A. The following are equivalent for all $x, y \in A$.

1. $x \sim y$ 2. $[x] = [y]$ 3. $[x] \cap [y] = \emptyset$

Theorem 8.3.4 The Partition induced by an Equivalence Relation

If A is a set and R is an equivalence relation on A, then the distinct equivalence classes of R form a partition of A; that is, the union of the equivalence classes is all of A, and the intersection of any two distinct classes is empty.

Definition: Divisiblity

$d | n \leftrightarrow \exists k \in \mathbb{Z}\ such\ that\ n = dk$

Definition: Congruence

Let $a, b \in \mathbb{Z}$ and $n \in Z^+$. Then **a is congruent to b modulo n** iff $a - b = nk$ for some $k \in \mathbb{Z}$. In other words, $n | (a - b)$.

$$a \equiv b (mod\ n)$$

Proposition: Congruence-mod n

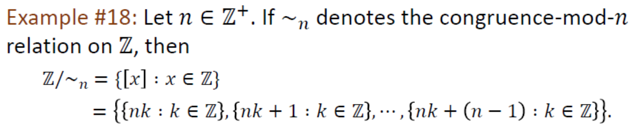
Congruence-mod n is an equivalence relation on $\mathbb{Z}$ for every $n \in \mathbb{Z}^+$

Definition: Set of equivalence classes

Let A be a set and ~ be an equivalence relation on A. Denote by A/~ the set of all equivalence classes with respect to ~, i.e.,

$$A\ /\sim\ = \{[x]_\sim : x \in A\}$$

We may read A/~ as "the quotient of A by ~"



Example #18: Let $n \in \mathbb{Z}^+$. If $\sim_n$ denotes the congruence-mod-n relation on $\mathbb{Z}$, then

$$\mathbb{Z}/\sim_n = \{[x] : x \in \mathbb{Z}\}$$
$$= \{\{nk : k \in \mathbb{Z}\}, \{nk + 1 : k \in \mathbb{Z}\}, \cdots, \{nk + (n-1) : k \in \mathbb{Z}\}\}.$$

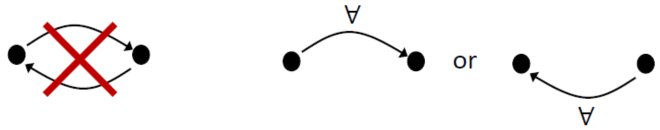
Theorem Rel.2 Equivalence classes form a partition

Let ~ be an equivalence relation on a set A. Then A/~ is a partition of A.

Definition: Antisymmetric

Let R be a relation on a set A. R is antisymmetric iff

$$\forall x, y \in A\ (xRy \wedge yRx \rightarrow x = y)$$



R is not antisymmetric iff $\exists x, y \in A\ (xRy \wedge yRx \wedge x \neq y)$

Note: antisymmetry != ~(symmetric)

Definition: Partial Order Relation

Let R be a relation defined on a set A. R is a partial order relation iff R is reflexive, antisymmetric, and transitive.

Note: $\leq$ *on* $\mathbb{R}$ and $\subseteq$ *on set of sets* are partial order relations.

Definition: Partially Ordered Set

A set A is called **partially ordered set (or poset)** with respect to a partial order relation R on A, denoted (A,R).

Theorem 4.3.3: Transitivity of Divisibility

For all integers a,b and c, $if\ a|b\ and\ b|c, then\ a|c$

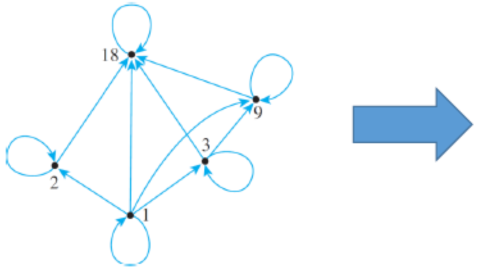
$|\ is\ a\ partial\ order\ relation\ on\ A \in \mathbb{Z}^+$

- We may view the set A as a set of tasks.
- Suppose $x, y \in A$. We write $x \preccurlyeq y$ iff task x must be done before or at same time as task y.
- For some elements x and y, it could be that neither $x \preccurlyeq y$ nor $y \preccurlyeq x$
- Hence the order is “partial”, that is there may not be an order between certain elements.

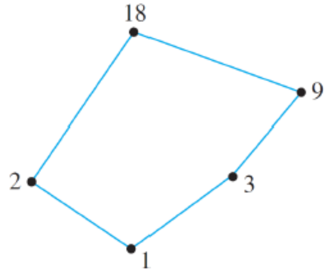
Hasse Diagrams

To obtain a Hasse diagram, start with a directed graph of the relation, placing vertices on the page so all arrows point upward. Then eliminate

- The loops at all vertices
- All arrows which existence is implied by transitive property
- The direction indicators on 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: Hasse Diagram

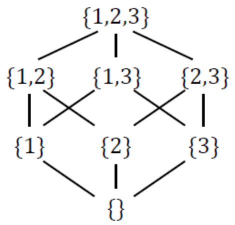
Let $\preccurlyeq$ be a partial order on a set A. A Hasse Diagram of $\preccurlyeq$ satisfies the following condition for all <u>distinct</u> $x, y, m \in A$:

> *If* $x \preccurlyeq$ y and no m ∈ A 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.*

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.

$\subseteq$ on $\wp(\{1,2,3\})$



Which of the following pairs of elements are comparable?

(a)	{1} and {1,3}	Yes
(b)	{2,3} and {2}	Yes
(c)	{1} and {3}	No
(d)	{1,2} and {3}	No
(e)	{3} and {1,2,3}	Yes

Theorem 6.4.5: Maximal/Minimal/Largest/Smallest Element
Let a set A be partially ordered with respect to a relation $\preccurlyeq$ and $c \in A$.

1. c is maximal element of A iff $\forall x \in A$, either x $\preccurlyeq$ c, or x and c are not comparable. Alternatively, c is a maximal element of A iff

$$\forall x \in A\ (c \preccurlyeq x \rightarrow c = x)$$

2. c is minimal element of A iff $\forall x \in A$, either c $\preccurlyeq$ x, or x and c are not comparable. Alternatively, c is a minimal element of A iff

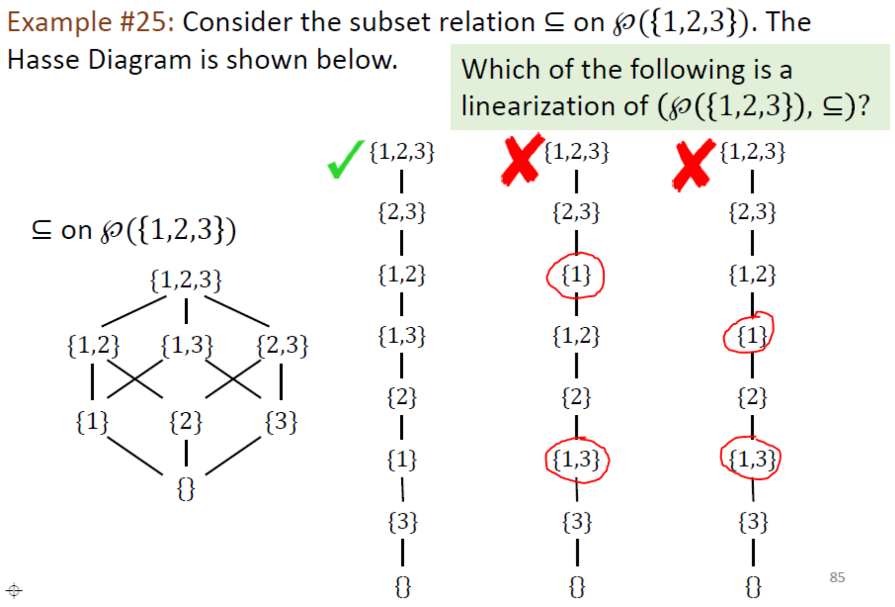
$$\forall x \in A\ (x \preccurlyeq c \rightarrow c = x)$$

3. c is the largest element of A iff $\forall x \in A(x \preccurlyeq c)$

4. c is the smallest element of A iff $\forall x \in A(c \preccurlyeq x)$

Proposition: A smallest element is minimal
Consider a partial order $\preccurlyeq$ on a set A.
Any smallest element is minimal.
Any largest element is maximal.

Linearization


Example #25: Consider the subset relation ⊆ on ℘({1,2,3}). The Hasse Diagram is shown below.

Which of the following is a linearization of (℘({1,2,3}), ⊆)?

Definition: Total Order Relations
When all elements of a partial order relation are comparable, the relation is called a total order (or linear order).

If R is a partial order relation on a set A, and for any two elements x and y in A, either xRy or yRx, then R is a total order relation (or simply total order) on A. In other words, R is a total order iff

$$\text{R is a partial order and } \forall x, y \in A(xRy \vee yRx)$$

Note: Divisibility relation | $on\ \mathbb{Z}^+$ is a partial order, but not a total order.

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

$$\forall x, y \in A\ (x \preccurlyeq y \rightarrow\ x \preccurlyeq^* y)$$

A linearization of a partial order can be seen as deriving one total order (among many possible total orders) from that partial order.

Kahn's Algorithm
Input: A finite set A and a partial order $\preccurlyeq$ on A.
```
1. $Set\ A_0 := A\ \ and\ i = 0$
2. $Repeat\ until\ A_i = \emptyset$
    2.1 $Find\ a\ minimal\ element\ c_i\ of\ A_i\ wrt\ \preccurlyeq$
    2.2 $set\ A_{i+1} = A_i \setminus \{c_i\}$
    2.3 $set\ i := i + 1$
```
Output: A linearization $\preccurlyeq^*$ of $\preccurlyeq$ defined by setting, for all indices i,j,

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

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.

$$\forall S \in \wp(A), S \neq \emptyset \rightarrow (\exists x \in S\ \forall y \in S\ (x \preccurlyeq y))$$

$(\mathbb{N}, \leq)$ is well-ordered
$(\mathbb{Z}, \leq)$ is not well-ordered

Common Mistakes

Statement: All birds can fly

$\forall x, \boldsymbol{Fly}(\boldsymbol{Bird}(x))$ This is like writing Fly(true) or Fly(false)

$\forall x, (\boldsymbol{Bird}(x) \wedge \boldsymbol{Fly}(x))$ Everything must be a bird and it flies

$\forall x, (\boldsymbol{Bird}(x) \rightarrow \boldsymbol{Fly}(x))$

Statement: There is a bird that can fly

$\exists x\ s.t. (\boldsymbol{Bird}(x) \rightarrow \boldsymbol{Fly}(x))$ What if there is no bird at all?

$\exists x\ s.t. (\boldsymbol{Bird}(x) \wedge \boldsymbol{Fly}(x))$

Which of the following are true, given the domain of x is non-empty?

(I) $\forall x\, P(x) \rightarrow \exists x\, P(x)$

(II) $\forall x (P(x) \wedge Q(x)) \equiv \forall x\, P(x) \wedge \forall x\, Q(x)$

(III) $\exists x\, (P(x) \wedge Q(x)) \rightarrow \exists x\, P(x) \wedge \exists x\, Q(x)$

(IV) $\exists x\, (P(x) \wedge Q(x)) \equiv \exists x\, P(x) \wedge \exists x\, Q(x)$

Relations

- FALSE > A relation that is symmetric cannot be antisymmetric.
- FALSE > A relation that is not symmetric must be antisymmetric.
- FALSE > In a partially ordered set, any minimal element is smallest.
- FALSE > In a partially ordered set, if there is exactly one minimal element, then there is a smallest element