Discrete Structures

Relations

Relations

A binary relation: Let A and B be sets. A binary relation R from A to B is a subset of $A \times B$ (Cartesian product). When (a, b) belong to R, a is said to be related to b by R.

Examples: parent-child, student-course

A n-ary relation: A relation R on sets $A_1, \dots, A_n$ is a subset of $A_1 \times \cdots \times A_n$

Note: In this course, we study binary relations. Then when we say a relation, we mean a binary relation.

Notation: We use notation $a\, R\, b$ to show $(a, b) \in R$ and $a \not R\, b$ to show $(a, b) \notin R$.

Functions as Relations

Let A and B be sets. A relation R from A to B can be used to express a one-to-many relationship between elements of A and B. A function f from A to B represent a relation where exactly one element of B is related to each element of A.

Relations are a generalization of functions; they can be used to express a much wider class of relationships between sets.

Relations on a Set

Definition: A relation on the set A is a relation from A to A.

Example: $\{(a, b): a|b\}$ which is a relation on integer numbers. We can name this relation |.

Example: $\{(a, b): a < b\}$ which is a relation on real numbers. We can name this relation $<$.

Example: $\{(A, B): A \subset B\}$ which is relation on the power set of a set X. We can name this relation $\subset$.

Problem: How many relations are there on a set A with n elements?

Solution: $A \times A$ has n^2 elements. Then we can have 2^{n^2} relations (#subsets)

Properties of Relations

Assumption: Assume R is a relation on a set A.

Reflexive: R is called reflexive iff $\forall a\ (aRa)$

Example: The "divide" relation is reflexive.

Symmetric: R is called symmetric iff $\forall a, b\ (aRb \rightarrow bRa)$

Antisymmetric: R is called antisymmetric iff $\forall a, b\ (aRb, bRa \rightarrow a = b)$

Example: The "divide" relation on positive integers is antisymmetric and is not symmetric.

Transitive: R is called transitive iff $\forall a, b, c\ (aRb\ \&\ bRc \rightarrow aRc)$

Example: The "divide" relation on integers is transitive.

Example: $R = \{(a, a): a \in A\}$ has all above properties.

Combining Relations

Set operations: As relations are subset of $A \times B$, Therefore, set operations like $\cup, \cap, -$ can be applied to them.

Composite of R and S: Let R be a relation from A to B and S be a relation from B to C. The composite of R and S, denoted by $\mathrm{S} \circ R$, is the following relation:

$$\mathrm{S} \circ R = \{(\mathrm{a}, \mathrm{c}) : \exists b\ aRb\ \&\ bSc\}$$

Example: $R = \{(1,1), (1,4), (2,3), (3,1), (3,4)\} \subset \{1,2,3\} \times \{1,2,3,4\}$ and $S = \{(1,0), (2,0), (3,1), (3,2), (4,1)\} \subset \{1,2,3,4\} \times \{0,1,2\}$, then $S \circ R = \{(1,0), (1,1), (2,1), (2,2), (3,0), (3,1)\}$

Combining Relations

Definition: Let R be a relation on A. The powers R^n are defined recursively by $R^1 = R, R^{n+1} = R^n \ o \ R$.

The definition shows $R^2 = R \ o \ R$, $R^3 = (R \ o \ R) \ o \ R$.

Theorem: The relation R on set A is transitive iff $R^n \subset R$ for any positive integer n

Proof:

If part: $R^n \subset R \rightarrow R^2 \subset R \rightarrow \forall a, b, c \ (aRb \ \& \ bRc \rightarrow aRc)$

Only if part: We use induction. Assume $R^n \subset R$. Now consider $R^{n+1} = R^n \ o \ R$. Assume $(a, b) \in R^{n+1}$. Then there is x s.t. $(a, x) \in R, (x, b) \in R^n$. Since $R^n \subset R$,and R is transitive then $(a, b) \in R$.

Representation of Relations

Using Matrix: Let R be a relation on $A = \{a_1, \dots, a_m\}$ and $B = \{b_1, \dots, b_n\}$. The relation R can be represented by the matrix $m \times n$ M_R where $m_{ij} = 1$ if $(a_i, b_j) \in R$ and $m_{ij} = 0$ if not.

Some Simple Observations:

- R is reflexive iff all elements on the main diagonal of M_R is 1.
- R is symmetric if M_R is a symmetric matrix
- $M_{R_1 \cup R_2} = M_{R_1} \vee M_{R_2}$ and $M_{R_1 \cap R_2} = M_{R_1} \wedge M_{R_2}$

Using Digraph: Let R be a relation on a set A. R can be modeled by a digraph G where each element of A is a vertex of G, and edge (a, b) exists in G iff $(a, b) \in R$.

Closure

Definition: Let R be a relation on a set A. R may or may not have some property P such as reflexivity or symmetry. If there is a relation S with property P containing R such that S is a subset of every relation with property P containing R, then S is called the closure of R with respect to P.

Example: Suppose $R = \{(1,1), (1,2), (2,1), (1,3)\}$ is a relation on $\{1,2,3\}$

- Reflexive closure: $\{(1,1), (2,2), (3,3), (1,2), (2,1), (1,3)\}$
- Symmetric closure: $\{(1,1), (1,2), (2,1), (1,3), (3,1)\}$
- Antisymmetric closure: does not exist
- Transitive closure: $= \{(1,1), (1,2), (2,1), (1,3), (2,3)\}$

Closure

Theorem: Let R be a relation on A. There is a path of length n where n is a positive integer, from a to b iff $(a, b) \in R^n$.

Proof:

- Proof is based on induction. Assume for n the claim is true. We show that the claim is true for $n + 1$
- $(a, b) \in R^{n+1} \leftrightarrow \exists c: (a, c) \in R^n \wedge (c, b) \in R \leftrightarrow \exists c$: there exists a path of length n from a to $c \wedge (c, b) \in R \leftrightarrow$ there exists a path of length $n + 1$ from a to b

Closure

Definition: Let R be a relation on A. The connectivity relation R^* consists of pairs (a, b) such that there is a path of length at least one from a to b in R.

Observation: $\cup_{i=1}^{\infty} R^i = R^*$

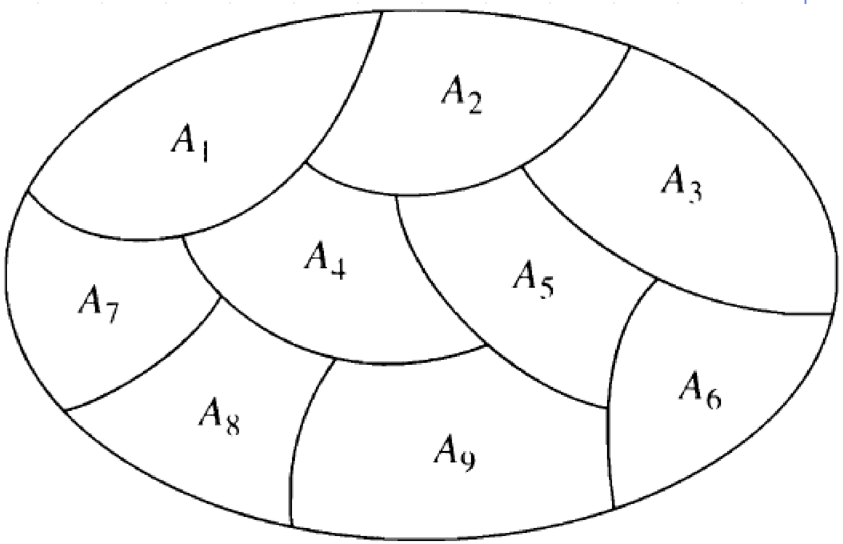
Theorem: The transitive closure of R is R^*.

Proof:

- R^* contains R and it is transitive.
- We show R^* is the subset of any transitive closure S of R.
- Since S is transitive, S^n is transitive and so $S^n \subset S$
- $S^* = \cup_{i=1}^{\infty} S^i \rightarrow S^* \subset S$
- $R \subset S \rightarrow R^* \subset S^*$
- Any transitive closure that contain R must also contain R^*. Therefore, $R^*$is the transitive closure

Equivalence Relations

Equivalence Relations: Let R be a relation on A. R is called an equivalence relation if it is reflexive, symmetric and transitive.



Equivalence Classes: For an equivalence relation R defined on a set A and $a \in A$, the class $[a] = \{\mathrm{b}: \mathrm{aRb}\}$

Theorem: Either $[a] = [b]$ or $[a] \cap [b] = \emptyset$

Proof:

- Assume $[a] \cap [b] \neq \emptyset$. Then $\exists c: aRc \wedge bRc$
- $x \in [a] \leftrightarrow aRx \wedge cRa \leftrightarrow cRx \wedge bRc \leftrightarrow bRx \leftrightarrow x \in [b]$
- Therefore $[a] = [b]$

Equivalence Relations

Example: For a given undirected graph $G(V,E)$, let $R = \{(u,v)$: there is a path from u to $v\}$. It is easy to see R is an equivalence relation. $[u]$ is the maximal connected component that u belongs to it. Indeed, classes are connected components.

Example: For a given directed graph $G(V,E)$, let $R = \{(u,v)$: there is a path from u to v and vice versa$\}$. It is easy to see R is an equivalence relation. $[u]$ is the maximal stongly connected component that u belongs to it. Indeed, classes are strongly connected components.

Equivalence Relations

Example: Let m be a positive integer greater than 1. The relation $R = \{(a, b) | \; a \equiv b \; mod \; m\}$ is an equivalence relation. Class $[a]$ is the set of all numbers congruent to a mod m. Integer numbers are partitioned into sets $[0], [1], \ldots, [m-1]$.

Example: Let S be the set of all strings. The relation $R = \{(s, t): |s| = |t|\}$ over S is an equivalence relation. Class $[s]$ is the set of all strings whose length is equal to the length of s. The strings are partitioned into equal-length strings.

Partial Orderings

Partial Ordering: A relation R on a set S is called a partial ordering or a partial order if it is reflexive, antisymmetric and transitive. A set S together with a partial order R is called a Partially Ordered Set (poset) and is denoted by (S, R). Members of S are called elements of poset.

Examples: relations $\leq, \subseteq, |$ are partial order

Notation: From now on, we use $\preccurlyeq$ to denote a partial order relation. So, a poset on S is denoted by $(S, \preccurlyeq)$

Comparable Elements

Definition: Two elements a and b of a poset $(S, \preccurlyeq)$ is comparable if either $a \preccurlyeq b$ or $b \preccurlyeq a$.

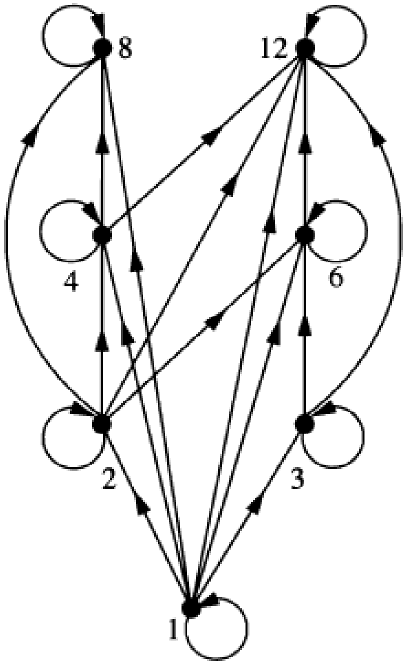
Examples: 2 and 3 are incomparable in $(Z^+, |)$ but 2 and 4 are comparable.

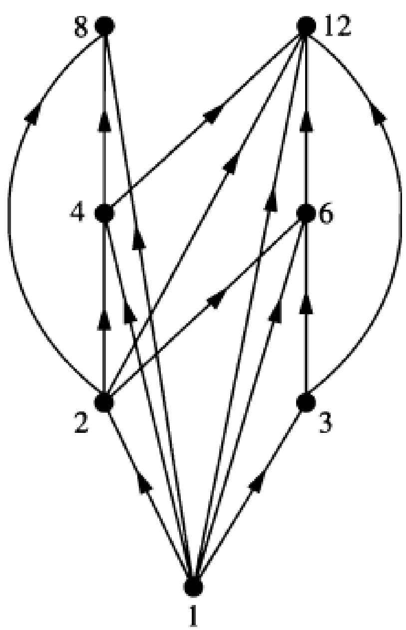
Remark: The adjective "partial" is used to describe partial ordering because pairs of elements may be incomparable. When every two elements in the set are comparable, the relation is called a total ordering. A totally ordered set is also called a chain. For instance $(Z, \leq)$ is a total order but $(Z^+, |)$ is not.

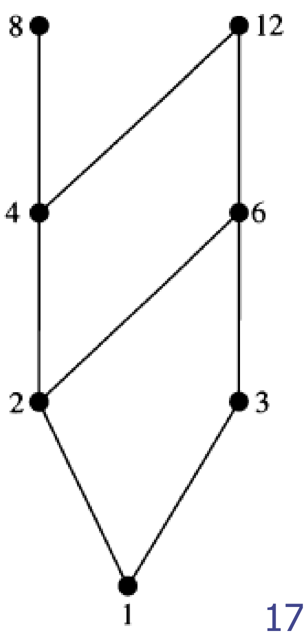
Hasse Diagrams

We can represent a poset using the following procedure

- Obtain the graph corresponding to the poset
- Arrange all edges such that the initial vertex is below the terminal vertex and remove all arrows
- Remove all self-loops
- Remove all edges which are present due to transitivity





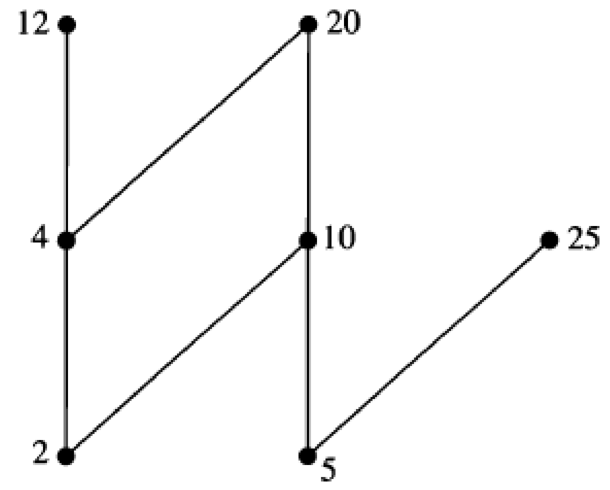


Maximal and Minimal

Maximal Elements: An element a in the poset is said to be maximal if there is no element b in the poset such that $a \prec b$

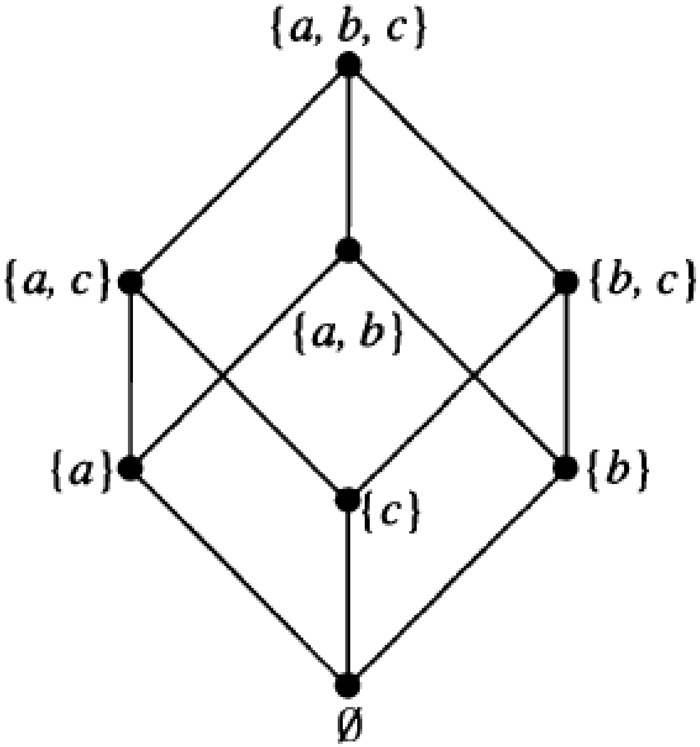
Minimal Elements: An element a in the poset is said to be minimal if there is no element b in the poset such that $b \prec a$

Maximal and minimal elements in the Hasse diagram are the topmost and bottommost elements, respectively.



Maximum and Minimum

- **Maximum Element or Greatest Element:** An element a in the poset is said to be maximum if for any element b in the poset we have $b \preccurlyeq a$
- **Minimum Element or Least Element:** An element a in the poset is said to be minimum if for any element b in the poset we have $a \preccurlyeq b$.

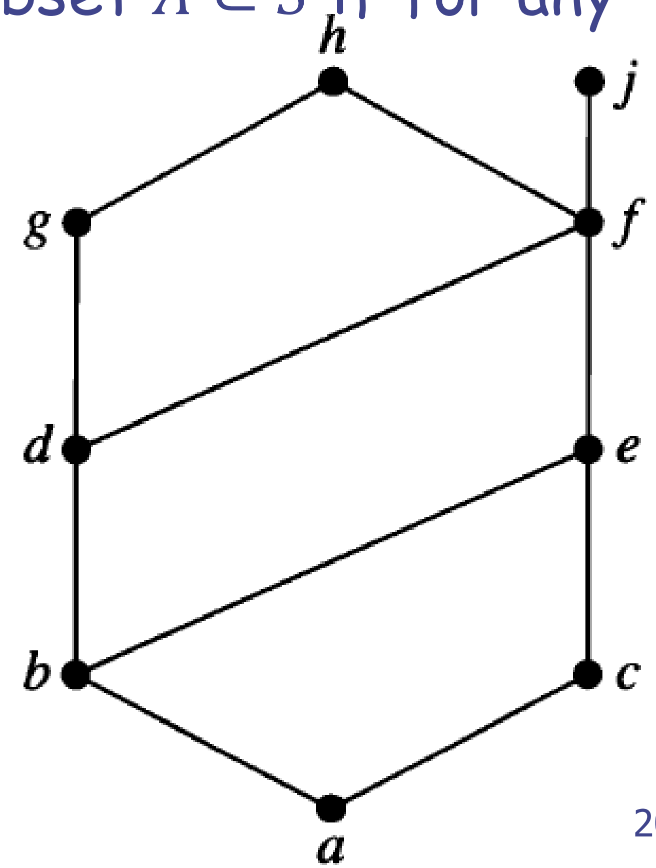


Upper and Lower Bounds

Upper Bound: An element b in the poset $(S, \preccurlyeq)$ is said to be a upper bound for the subset $A \subset S$ if for any $a \in A$ we have $a \preccurlyeq b$.

Lower Bound: An element b in the poset $(S, \preccurlyeq)$ is said to be a lower bound for the subset $A \subset S$ if for any $a \in A$ we have $b \preccurlyeq a$.

Example: Upper bounds of $\{a, c, d, f\}$ are f, h and j and the lower bound is a.
The set $\{j, h\}$ does not have any upper bound.



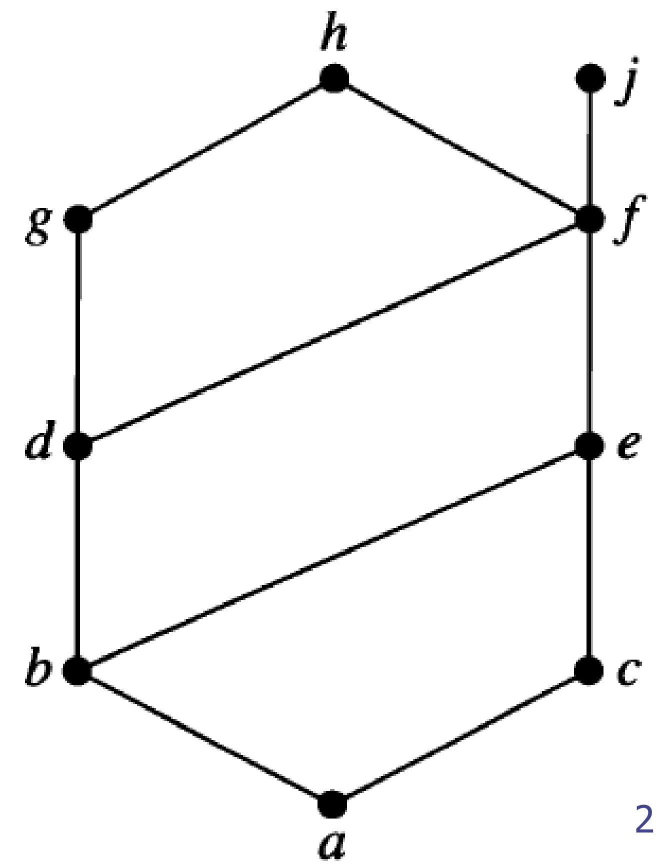
Upper and Lower Bounds

Least Upper Bound (LUB): An upper bound which is less than any upper bound.

Greatest Lower Bound (GLB): A lower bound which is greater than any lower bound.

Example: LUB of $\{a, c, d, f\}$ is f and its GLB is a

.



Lattice

Lattice: A Poset $(S, \preccurlyeq)$ in which every pair of elements has both, a least upper bound and a greatest lower bound is called a lattice.

Operators: $a \uparrow b = LUB(a, b)$ and $a \downarrow b = GLB(a, b)$

Properties:

1. $a \uparrow a = a \downarrow a = a$
2. $a \uparrow b = b \uparrow a, a \downarrow b = b \downarrow a$
3. $(a \uparrow b) \uparrow c = a \uparrow (b \uparrow c), (a \downarrow b) \downarrow c = a \downarrow (b \downarrow c)$
4. Distributive law may or may not hold for a lattice $(a \uparrow (b \downarrow c) = (a \uparrow b) \downarrow (a \uparrow c), a \downarrow (b \uparrow c) = (a \downarrow b) \uparrow (a \downarrow c))$

Lattice

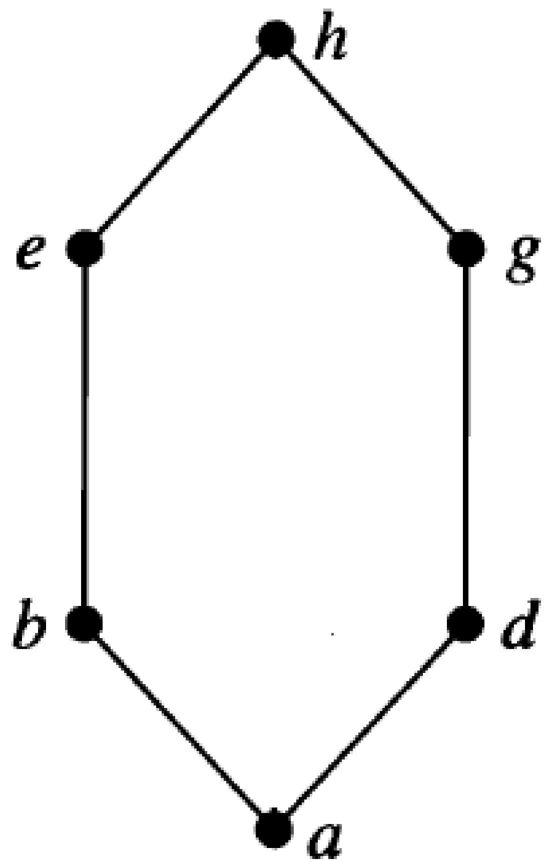
Proof of $(a \uparrow b) \uparrow c = a \uparrow (b \uparrow c)$:

- Let $(a \uparrow b) \uparrow c = \mathrm{d}$, $a \uparrow (b \uparrow c) = \mathrm{d}'$
- We show $d \preccurlyeq d'$and similarly $d' \preccurlyeq d$.
- We know $a \preccurlyeq d'$ and $b \uparrow c \preccurlyeq d'$
- So $a \preccurlyeq d'$, $b \preccurlyeq d'$, $c \preccurlyeq d'$
- So $a \uparrow b \preccurlyeq \mathrm{d}'$ and $c \preccurlyeq d'$
- So $(a \uparrow b) \uparrow c \preccurlyeq d'$
- Therefore, $d \preccurlyeq d'$

Lattice

Counter Example for Distributive Law:

- $b \uparrow (e \downarrow g) = b \uparrow a = b$
- $(b \uparrow e) \downarrow (b \uparrow g) = \text{e} \downarrow h = e$



Lattice

Example: $(Z^+, |)$ is a lattice. Here $a \uparrow b = [\mathrm{a}, \mathrm{b}]$ and $a \downarrow b = (\mathrm{a}, \mathrm{b})$

Example: $(P(X), \subseteq)$ is a lattice where $P(X)$ is the power set of a set X. Here $A \uparrow B = A \cup B, A \downarrow B = A \cap B$

Example: $(Z, \leq)$ is a lattice. Here $a \uparrow b = max(a, b)$, $a \downarrow b = \min(a, b)$

Boolean Algebra

A Boolean Algebra is a six tuple consisting of a set A, equipped with two binary operations $\wedge$ and $\vee$, a unary operation $\sim$, and two element 0 and 1 in A such that for all elements a, b and c of A, the following axioms hold:

- Associativity: $a \vee (b \vee c) = (a \vee b) \vee c$ and $a \wedge (b \wedge c) = (a \wedge b) \wedge c$
- Commutativity: $a \vee b = b \vee a$ *and* $a \wedge b = b \wedge a$
- Identity: $a \vee 0 = a$ *and* $a \wedge 1 = a$
- Distributivity: $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ and $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
- Complements: $a \vee \sim a = 1$ and $a \wedge \sim a = 0$

Boolean Algebra is a complemented distributive lattice.

Set and proposition logic are two examples.