Mathematical Induction

Principle of Mathematical Induction

- An example of inductive proof:

  Show that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ is true for all $n \in \mathbf{Z}^+$.

  The inductive proof consists of two parts.

  First, we show that the statement is true for the base case, i.e., for $n = 1$.

  Second, we assume that the statement is true for n, and then show that it is also true for $n + 1$.

- Does $\mathbf{Z}^+$ have any distinct property against $\mathbf{Q}^+$ and $\mathbf{R}^+$?

$$\mathbf{Z}^+ = \{x \in \mathbf{Z} \mid x > 0\} = \{x \in \mathbf{Z} \mid x \geq 1\}$$

$$\mathbf{Q}^+ = \{x \in \mathbf{Q} \mid x > 0\}, \qquad \mathbf{R}^+ = \{x \in \mathbf{R} \mid x > 0\}$$

- The well-ordering principle:

  Every nonempty subset of $\mathbf{N}$ contains a smallest element

  ($\mathbf{N}$ is well-ordered)

  - Can be used to prove the principle of mathematical induction
  - $\mathbf{R}^+$ is not well-ordered

- Theorem: The Principle of Mathematical Induction

  Let $P(n)$ be a proposition for a natural number n.

  - If $P(0)$ is true; and
  - If $(\forall k \in \mathbf{N})\ (P(k) \rightarrow P(k+1))$ is true;

  Then, $(\forall n \in \mathbf{N})\ P(n)$ is true

- Consider applying the Modus Ponens

$$
\begin{array}{ll}
P(0) & \\
P(0) \rightarrow P(1) & P(1) \\
P(1) \rightarrow P(2) & P(2) \\
\quad \cdots\cdots & \quad \cdots \\
P(k) \rightarrow P(k+1) & P(k+1)
\end{array}
$$

Proof (by contradiction):

Suppose $(\forall n \in \mathbf{N})\ P(n)$ is not true.

If we let $F = \{t \in \mathbf{N} \mid P(t) \text{ is false}\}$, $F \neq \varnothing$.

Then, there must be a smallest element $s \in F$ by the well-ordering principle. Notice that $P(s)$ is false.

Since $P(0)$ is true, $s \neq 0$.

So, $s > 0$ and thus $s - 1 \in \mathbf{N}$.

With $s - 1 \notin F$ we have $P(s - 1)$ true.

Therefore, $P((s - 1) + 1) = P(s)$ is true, which is a contradiction.

Examples

- For all $n \in \mathbf{Z}^+$,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Proof:

(Basis step) For $n = 1$

LHS = 1, RHS = 1. So, LHS = RHS.

(Inductive step)

We want to show that

$$(\forall n \in \mathbf{N}) \quad \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \quad \Rightarrow \quad \sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$$

Proof:

Let $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ (Additional premise, or Inductive Hypothesis)

Then,

$$\sum_{i=1}^{n+1} i = (n+1) + \sum_{i=1}^{n} i$$

$$= (n+1) + \frac{n(n+1)}{2}$$ (by the inductive hypothesis)

$$= \frac{2(n+1) + n(n+1)}{2}$$

$$= \frac{(n+1)(n+2)}{2}$$

***Proof*:**

By applying the CP rule, we get

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \quad \Rightarrow \quad \sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$$

Since our choice of n for the inductive hypothesis was arbitrary,

$$(\forall n \in \mathbf{N}) \quad \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \quad \Rightarrow \quad \sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2} \qquad \text{(UG)}$$

- Let $r \neq 0$ and $r \neq 1$

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}$$

Proof:

(Basis step) For $n = 0$

LHS = 1, RHS = 1. So, LHS = RHS.

(Inductive step)

Let $\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}$ (AP, i.e., Inductive Hypothesis)

Proof:

We want to show that $\sum_{i=0}^{n+1} r^i = \frac{r^{n+2}-1}{r-1}$

(and we will apply the CP rule)

$$\sum_{i=0}^{n+1} r^i = r^{n+1} + \sum_{i=0}^{n} r^i$$

$$= r^{n+1} + \frac{r^{n+1}-1}{r-1}$$ (by the Inductive Hypothesis)

$$= \frac{r^{n+2}-r^{n+1}+r^{n+1}-1}{r-1} = \frac{r^{n+2}-1}{r-1}$$

- For all $n \in \mathbf{Z}^+$,

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Proof:

(Basis step) For $n = 1$

LHS = 1, RHS = 1. So, LHS = RHS.

(Inductive step)

Let $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ (Inductive Hypothesis)

We want to show that $\sum_{i=1}^{n+1} i^2 = \frac{(n+1)(n+2)(2n+3)}{6}$

Proof:

$$\sum_{i=1}^{n+1} i^2 = (n+1)^2 + \sum_{i=1}^{n} i^2$$

$$= (n+1)^2 + \frac{n(n+1)(2n+1)}{6}$$ (by the Inductive Hypothesis)

$$= \frac{6(n+1)^2 + n(n+1)(2n+1)}{6} = \frac{(n+1)[6(n+1) + n(2n+1)]}{6}$$

$$= \frac{(n+1)(2n^2 + 7n + 6)}{6} = \frac{(n+1)(n+2)(2n+3)}{6}$$

- For every $n \in \mathbf{N}$, $7^n - 2^n$ is divisible by 5.

Proof:

(Basis step) For $n = 0$

$7^0 - 2^0 = 0$ is divisible by 5.

(Inductive step)

Let $7^n - 2^n$ be divisible by 5.

Then,

$$7^{n+1} - 2^{n+1} = 7\cdot(7^n - 2^n) + 7\cdot 2^n - 2^{n+1}$$

$$= 7\cdot(7^n - 2^n) + 2^n\cdot(7 - 2)$$

Proof:

Since $(7^n – 2^n)$ is divisible by 5 by the inductive hypothesis, $7·(7^n – 2^n)$ is divisible by 5.

Also, $2^n·(7– 2)$ is divisible by 5.

Therefore, $7^{n+1} – 2^{n+1}$ is divisible by 5.

- If S is a finite set then $|\wp(S)| = 2^{|S|}$.

Proof:

(Basis step) For $S = \varnothing$

LHS $= |\wp(\varnothing)| = |\{\varnothing\}| = 1 = 2^0 = 2^{|\varnothing|} =$ RHS.

(Inductive step)

Let $|\wp(S)| = 2^{|S|} = 2^n$ for $S = \{a_1, a_2, \ldots, a_n\}$.

We want to prove that $|\wp(S')| = 2^{|S'|} = 2^{n+1}$

where $S' = \{a_1, a_2, \ldots, a_n, a_{n+1}\}$.

Proof:

We know that if $X \subseteq S$ then $X \subseteq S'$, which means that every subset of S is a subset of S'.

But, note that $X \cup \{a_{n+1}\} \subseteq S'$ for any $X \subseteq S$ and there is no other subset of S' in addition to these subsets.

Therefore, the number of subsets of S' is twice that of S, i.e.,

$$|\wp(S')| = 2\cdot|\wp(S)| = 2\cdot 2^{|S|} = 2\cdot 2^{n} = 2^{n+1} = 2^{|S'|}.$$

- The number of left parenthesis is equal to the number of right parenthesis in a propositional well-formed formula.

Proof:

Let $\#L(\mathbf{F})$ and $\#R(\mathbf{F})$ denote the number of left parenthesis and the number of right parenthesis of a wff $\mathbf{F}$, respectively.

(Basis Step)

Since any propositional variable or constant S has no parenthesis by the basis clause of the inductive definition of a wff, $\#L(S) = \#R(S)$.

Proof:

(Inductive Step)

Let P and Q be two wffs such that

$$\#L(P) = \#R(P) \text{ and } \#L(Q) = \#R(Q).$$

Let $\mathbf{F}$ be any one of the formulas defined by the inductive clause of the inductive definition of a wff, that is, $(\neg P)$, $(P \vee Q)$, $(P \wedge Q)$, $(P \to Q)$, and $(P \leftrightarrow Q)$.

If $\mathbf{F} = (\neg P)$, then $\#L(\mathbf{F}) = \#L(P) + 1$ and $\#R(\mathbf{F}) = \#R(P) + 1$.

Therefore, $\#L(\mathbf{F}) = \#R(\mathbf{F})$.

Proof:

On the other hand, if $\mathbf{F}$ is $(P \vee Q)$, $(P \wedge Q)$, $(P \rightarrow Q)$, or $(P \leftrightarrow Q)$, then

$\#L(\mathbf{F}) = \#L(P) + \#L(Q) + 1$ and

$\#R(\mathbf{F}) = \#R(P) + \#R(Q) + 1$.

Again, since $\#L(P) = \#R(P)$ and $\#L(Q) = \#R(Q)$,

$\#L(\mathbf{F}) = \#R(\mathbf{F})$.

Closures

Example:

Let $A = \{a, b, c\}$ and $R = \{(a, b), (c, a)\}$. To make R reflexive, we need to add at least three tuples (a, a), (b, b), and (c, c).

- Definition:

If R is a relation on a set A then the reflexive (symmetric, transitive) closure of R is a relation R' such that

1. R' is reflexive (symmetric, transitive)
2. $R \subseteq R'$
3. If R'' is another reflexive (symmetric, transitive) relation such that $R \subseteq R''$, then $R' \subseteq R''$.

- Notations:

  Reflexive, symmetric, and transitive closure of R will be denoted by $r(R)$, $s(R)$, and $t(R)$, respectively.

- Theorem: Let R be a relation on a set A. Then,

  (a) $r(R) = R \cup E_A$.

  (b) $s(R) = R \cup R^c$.

  (c) $t(R) = \bigcup_{i=1}^{\infty} R^i$.

Proof of (a) $r(R) = R \cup E_A$

1. $R \cup E_A$ is obviously reflexive.
2. $R \subseteq R \cup E_A$
3. Let R'' be a reflexive relation such that $R \subseteq R''$.

   We need to show that $R \cup E_A \subseteq R''$.

   Since R'' is reflexive, $E_A \subseteq R''$.

   But $R \subseteq R''$, and thus $R \cup E_A \subseteq R''$.

Since $R \cup E_A$ satisfies all the three conditions in the definition of the reflexive closure of R, $R \cup E_A$ is the reflexive closure of R, i.e., $r(R) = R \cup E_A$. □

Proof of (b) $s(R) = R \cup R^c$

1. $R \cup R^c$ is symmetric because for every $(x, y) \in R \cup R^c$, $(y, x) \in R \cup R^c$.
2. $R \subseteq R \cup R^c$
3. Let R'' be a symmetric relation on A such that $R \subseteq R''$.

   We must show that $R \cup R^c \subseteq R''$.

   $R \subseteq R''$ is given.

   Since R'' is symmetric, $R^c \subseteq R''$.

   - Let $(x, y) \in R^c$. Then $(y, x) \in R$.

     Since $R \subseteq R''$, $(y, x) \in R''$.

     But, R'' is symmetric and so $(x, y) \in R''$.

     Therefore, $R^c \subseteq R''$. $\square$

- Lemma: Let R be a relation on a set A. Then,

$$R^n \subseteq t(R), \text{ for all } n \geq 1.$$

Proof of lemma:

(Basis Step) For $n = 1$,

$R \subseteq t(R)$ by the definition of $t(R)$.

(Inductive step)

Assume $R^n \subseteq t(R)$.

We want to prove that $R^{n+1} \subseteq t(R)$.

Note that $R^{n+1} = R \circ R^n$.

Proof of lemma:

Since $R \subseteq t(R)$, $R^n \subseteq t(R)$, and $t(R)$ is transitive, $R \circ R^n \subseteq t(R)$.

- Let $(x, z) \in R \circ R^n$.

  There must exist a y such that $(x, y) \in R$ and $(y, z) \in R^n$.

  But $R \subseteq t(R)$ and $R^n \subseteq t(R)$.

  Hence $(x, y) \in t(R)$ and $(y, z) \in t(R)$.

  Since $t(R)$ is transitive, $(x, z) \in t(R)$.

  Therefore, $R \circ R^n \subseteq t(R)$.

Therefore, $R^n \subseteq t(R)$ for all $n \geq 1$. □

Proof of (c) $t(R) = \bigcup_{i=1}^{\infty} R^i$

By the previous lemma $R^n \subseteq t(R)$ for all $n \geq 1$.

Thus, $\bigcup_{i=1}^{\infty} R^i \subseteq t(R)$.

Now we must show that $t(R) \subseteq \bigcup_{i=1}^{\infty} R^i$.

Obviously, $R \subseteq \bigcup_{i=1}^{\infty} R^i$.

All that remains to be shown now is that $\bigcup_{i=1}^{\infty} R^i$ is transitive.

Let $(x, y) \in \bigcup_{i=1}^{\infty} R^i$ and $(y, z) \in \bigcup_{i=1}^{\infty} R^i$.

Since $(x, y) \in \bigcup_{i=1}^{\infty} R^i$, there must exist an s such that $(x, y) \in R^s$.

Similarly, there must exist a t such that $(y, z) \in R^t$.

Then, $(x, z) \in R^s \circ R^t = R^{s+t}$ and $R^{s+t} \subseteq \bigcup_{i=1}^{\infty} R^i$.

Thus, $(x, z) \in \bigcup_{i=1}^{\infty} R^i$.

Therefore, $\bigcup_{i=1}^{\infty} R^i$ is transitive. □

- Theorem: Let R be a binary relation. Then,
  - (a) R is reflexive iff $r(R) = R$.
  - (b) R is symmetric iff $s(R) = R$.
  - (c) R is transitive iff $t(R) = R$.

Proof of (a)

(if part): R is reflexive if $r(R) = R$.

Assume $r(R) = R$.

Since the reflexive closure is reflexive, R is obviously reflexive.

Proof of (a)

(only if part): R is reflexive only if $r(R) = R$.

Assume R is reflexive.

Since $R \subseteq R$ and R is reflexive, $r(R) \subseteq R$ by the definition of the reflexive closure.

But $R \subseteq r(R)$ also by the definition of the reflexive closure.

Therefore, $R = r(R)$. $\square$

- **Theorem:** Let R be a binary relation.
  - (a) If R is reflexive then so are $s(R)$ and $t(R)$.
  - (b) If R is symmetric then so are $r(R)$ and $t(R)$.
  - (c) If R is transitive then so is $r(R)$.

Example:

$R = \{(a, b)\}$ is transitive.

$s(R) = R \cup R^c = \{(a, b), (b, a)\}$ is not transitive.

Proof of (a)

Assume R is a reflexive relation.

We prove that $s(R)$ is reflexive.

Since R is reflexive, $E \subseteq R$.

We know by the definition of $s(R)$ that $R \subseteq s(R)$.

Thus, $E \subseteq s(R)$.

Therefore, $s(R)$ is reflexive.

We can similarly show that $t(R)$ is reflexive.

$\square$

- Theorem: Let R be a binary relation.
  - (a) $rs(R) = sr(R)$.
  - (b) $rt(R) = tr(R)$.
  - (c) $st(R) \subseteq ts(R)$.

Proof of (a)

$$
\begin{aligned}
rs(R) &= r(R \cup R^c) \\
&= R \cup R^c \cup E = R \cup R^c \cup E \cup E = R \cup R^c \cup E \cup E^c \\
&= (R \cup E) \cup (R^c \cup E^c) \\
&= (R \cup E) \cup (R \cup E)^c \\
&= s(R \cup E) \\
&= sr(R) \quad \Box
\end{aligned}
$$

- Lemma: Let R_1 and R_2 be two relations.

  If $R_1 \subseteq R_2$, then $s(R_1) \subseteq s(R_2)$ and $t(R_1) \subseteq t(R_2)$.

Proof of (c) $st(R) \subseteq ts(R)$

$R \subseteq s(R)$ by the definition of the closure.

$t(R) \subseteq ts(R)$ by the above lemma.

$st(R) \subseteq sts(R)$ again by the above lemma.

Since $s(R)$ is symmetric, $ts(R)$ is symmetric by the previous theorem.

Proof of (c) $st(R) \subseteq ts(R)$

Since $ts(R)$ is symmetric, it must be equal to its symmetric closure, by one of the previous theorems.

Hence, $sts(R) = ts(R)$.

Therefore $st(R) \subseteq ts(R)$. □

- A counter example for $ts(R) \subseteq st(R)$.

Let $R = \{(a, b)\}$.

Then, $t(R) = \{(a, b)\}$ and $st(R) = \{(a, b), (b, a)\}$.

Also, $s(R) = \{(a, b), (b, a)\}$ and $ts(R) = \{(a, b), (b, a), (a, a), (b, b)\}$.

We can see that $ts(R) \not\subseteq st(R)$.

Partial Orderings, Lattices, and Boolean Algebra

Partial Orderings

- Definition:

  A binary relation R on a set is called a partial ordering if it is reflexive, antisymmetric, and transitive.

Example:

- “refines” is a partial ordering on the set of all the partitions.

- Notation:

  $\leq$ is used as a generic symbol for partial ordering.

  E.g., let $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$.

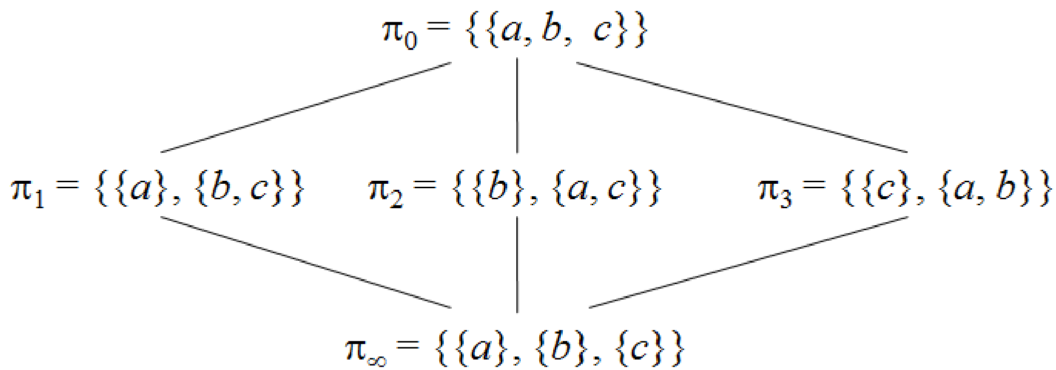
  Consider “divides” relation on A: x divides y if x is a factor of y.

  ➡ $2 \leq 6$ and $3 \leq 6$ are true but $5 \leq 6$ is not true.

- Definition:

  When R is a partial ordering on a set A, the pair (A, R) is called a partially ordered set or a poset.

- Examples of posets:
  - $(\mathbf{R}, \leq)$
  - (the set of all the partitions, refines)
  - ($\mathbf{Z}^+$, divides)
  - $(\wp(A), \subseteq)$



- Theorem:

  If R is a partial ordering on a set A, then R^c is also a partial ordering on A.

- Definition:

  Let R be a partial ordering on a set A and let $X \subseteq A$. The restriction of R on X, denoted R/X, is defined by

$$R/X = \{(x, y) \mid x \in X \wedge y \in X \wedge (x, y) \in R\}$$

<u>Example</u>:

$A = \mathbf{Z}^+$ $\qquad X = \{1, 2, 3, 4, 5, 6, 7\}$

- divides/X = $\{(1, 1), (1, 2), \ldots, (1, 7), (2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4), (5, 5), (6, 6), (7,7)\}$

- Theorem:

  Let R be a partial ordering on a set A and let $X \subseteq A$. Then R/X is a partial ordering on X.

- Definition:

  Let R be a partial ordering on a set A. If $a, b \in A$ are such that either $(a, b) \in R$ or $(b, a) \in R$ then a and b are said to be comparable.

<u>Example</u>:

$A = \{a, b, c\}$ $\qquad$ $R = \{(a, a), (b, b), (c, c), (a, b)\}$

- a and b are comparable.
- a and c are not comparable. b and c are not comparable.

- **Definition**:

  Let R be a partial ordering on a set A such that every pair $a, b \in A$ is comparable. Then R is said to be a linear ordering (total ordering) and (A, R) is said to be a linearly ordered set (totally ordered set) or a chain.

- **Definition**:

  A relation R on a set A is called a strict partial ordering if it is irreflexive, asymmetric, and transitive.

<u>Example</u>:

$A = \{a, b, c\}$ $\qquad$ $R = \{(a, a), (b, b), (c, c), (a, b)\}$

- $R' = \{(a, b)\}$ is a strict partial ordering

- Notation:

  $<$ is used as a generic symbol for strict partial ordering.

  $< \, = \{(x, y) \mid (x, y) \in \, \leq \wedge \, x \neq y\} = \, \leq - E_A$

- Definition:

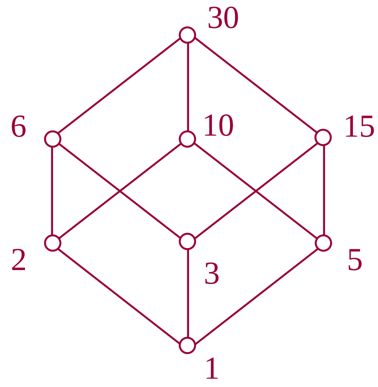
  Let $<$ be a strict partial ordering on a set A. Then the covers relation with respect to $<$ on A, denoted by $covers_<$, is defined as follows:

  $covers_< = \{(x, y) \mid y < x$ and there is no z such that $y < z$ and $z < x\}$

Example:

- "divides" relation on $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$
- $< \; = \; \leq - E_A$

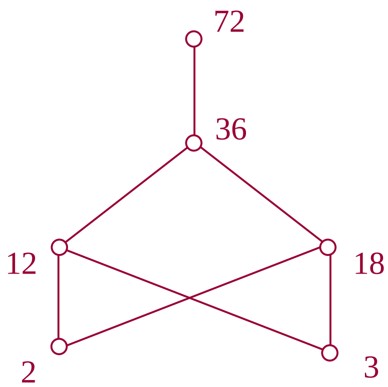
  $= \{(1, 2), \ldots, (1, 30), (2, 6), (2, 10), (2, 30), (3, 6), (3, 15), (3, 30),$
  $(5, 10), (5, 15), (5, 30), (6, 30), (10, 30), (15, 30)\}$
- $covers_< = \{(30, 15), (30, 10), (30, 6), (15, 5), (15, 3), (10, 5), (10, 2),$
  $(6, 3), (6, 2), (5, 1), (3, 1), (2, 1)\}$



Hasse Diagram

Example:

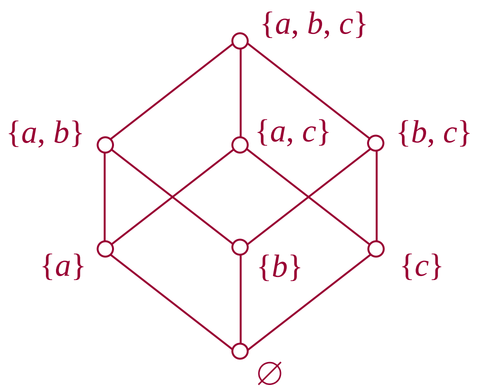
- “divides” relation on $A = \{2, 3, 12, 18, 36, 72\}$
- $< = \{(2, 12), (2, 18), (2, 36), (2, 72), (3, 12), (3, 18), (3, 36), (3, 72),$
  $(12, 36), (12, 72), (18, 36), (18, 72), (36, 72)\}$
- $covers_< = \{(72, 36), (36, 18), (36, 12), (18, 3), (18, 2), (12, 3), (12, 2)\}$



We can restore ≤ from the Hasse diagram.

Example:

- $(\wp(A), \subseteq)$ where $A = \{a, b, c\}$
- $covers_{<} = \{(\{a, b, c\}, \{a, b\}), (\{a, b, c\}, \{a, c\}), (\{a, b, c\}, \{b, c\}),$
  $(\{a, b\}, \{a\}), (\{a, b\}, \{b\}), (\{a, c\}, \{a\}), (\{a, c\}, \{c\}),$
  $(\{b, c\}, \{b\}), (\{b, c\}, \{c\}), (\{a\}, \varnothing), (\{b\}, \varnothing), (\{c\}, \varnothing)\}$



Example:

- "less than or equal to" relation on $A = \{1, 2, 3, 4, 5\}$
- This relation is a linear ordering.
- The poset is called a linearly ordered set, totally ordered set, or chain.

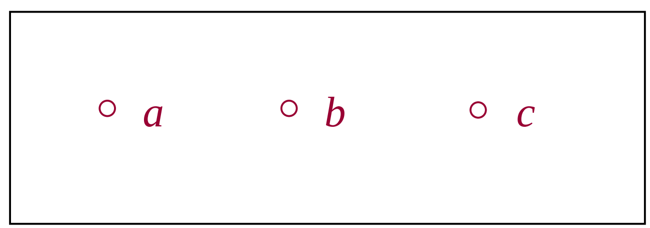
Example:

- Consider the Identity relation E_A on $A = \{a, b, c\}$
- This relation is
  - reflexive
  - symmetric
  - antisymmetric
  - transitive

equivalence relation

partial ordering

Hasse diagram of E_A:



Bounds

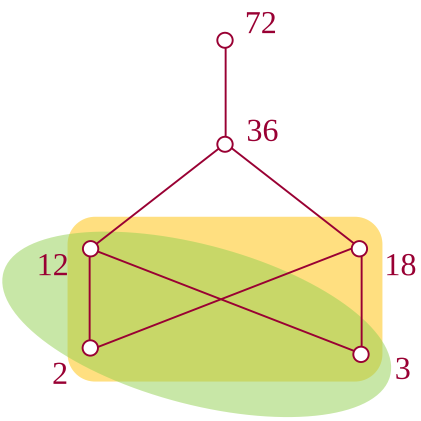
- Definition:

  Let $(A, \leq)$ be a poset and let $X \subseteq A$. Then,

  - $a \in X$ is the greatest element of X if $x \leq a$ for every $x \in X$.
  - $a \in X$ is the least element of X if $a \leq x$ for every $x \in X$.
  - $a \in X$ is the maximal element of X if there is no $x \in X$ such that $a < x$.
  - $a \in X$ is the minimal element of X if there is no $x \in X$ such that $x < a$.

Example:

- "divides" relation on $A = \{2, 3, 12, 18, 36, 72\}$
- $X_1 = \{2, 3, 12\}$
  - greatest element of X_1: 12
  - least element of X_1: none
- $X_2 = \{2, 3, 12, 18\}$
  - greatest element of X_2: none
  - least element of X_2: none



- Theorem:

  Let $(A, \leq)$ be a poset and let $X \subseteq A$. Then the greatest (least) element of X if it exists is unique.

Proof:

Let there be two elements a and b that are the greatest elements of X.

Then, $a \leq b$ because b is the greatest element of X and $a \in X$.

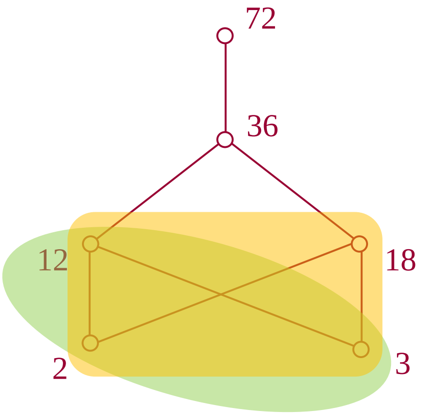
Similarly, $b \leq a$ because a is the greatest element of X and $b \in X$.

From $a \leq b$ and $b \leq a$, we conclude $a = b$ because $\leq$ is antisymmetric.

□

Example:

- "divides" relation on $A = \{2, 3, 12, 18, 36, 72\}$
- $X_1 = \{2, 3, 12\}$
  - maximal element of X_1: 12
  - minimal element of X_1: 2, 3
- $X_2 = \{2, 3, 12, 18\}$
  - maximal element of X_2: 12, 18
  - minimal element of X_2: 2, 3



- Theorem:

  Let $(A, \leq)$ be a poset and let $X \subseteq A$. If $a \in X$ is the unique maximal (minimal) element of X then a is the greatest (least) element of X.

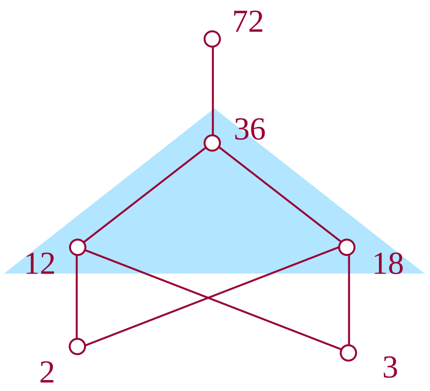
- Definition:

  Let $(A, \leq)$ be a poset and let $X \subseteq A$. Then,

  - $a \in A$ is the upper bound of X if $x \leq a$ for every $x \in X$.
  - $a \in A$ is the lower bound of X if $a \leq x$ for every $x \in X$.

Example:

- “divides” relation on $A = \{2, 3, 12, 18, 36, 72\}$
- $X = \{12, 18, 36\}$
  - greatest element: 36
  - least element: none
  - maximal element: 36
  - minimal element: $12, 18$
  - upper bound: $36, 72$
  - lower bound: $2, 3$



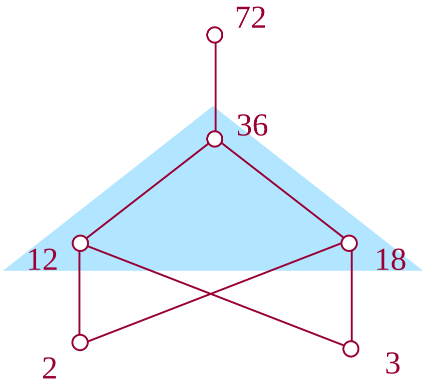
- Definition:

  Let $(A, \leq)$ be a poset and let $X \subseteq A$. Then,

  - The least element of the set of upper bounds of X is called the least upper bound (LUB, supremum) of X.
  - The greatest element of the set of lower bounds of X is called the greatest lower bound (GLB, infimum) of X.

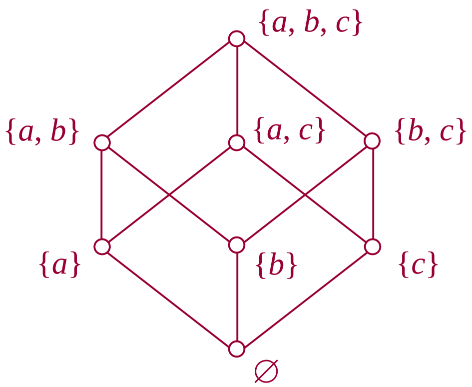
Example:

- "divides" relation on $A = \{2, 3, 12, 18, 36, 72\}$
- $X = \{12, 18, 36\}$
  - LUB of X: 36
  - GLB of X: none



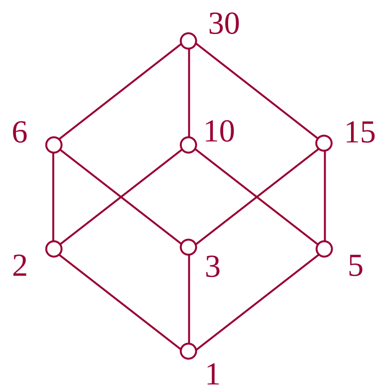
Example:

- Consider the poset $(\wp(A), \subseteq)$ where $A = \{a, b, c\}$.
- Let $X_i, X_j \in \wp(A)$. Then,
  - LUB of $\{X_i, X_j\} = X_i \cup X_j$
  - GLB of $\{X_i, X_j\} = X_i \cap X_j$



Example:

- Consider the poset $(A, \text{divides})$ where $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$.
- Let $a, b \in A$. Then,
  - LUB of $\{a, b\}$ = LCM (Least Common Multiple) of a and b
  - GLB of $\{a, b\}$ = GCD (Greatest Common Divisor) of a and b



Isomorphism

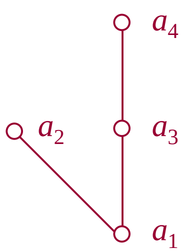
- Definition:

  Let $(A, \leq)$ and $(B, \leq')$ be two posets and let $f : A \to B$. The function f is said to be order preserving with respect to $\leq$ and $\leq'$ if and only if for every $x, y \in A$ if $x \leq y$ then $f(x) \leq' f(y)$.

Example:

- $f: A \to B$

  $A = \{a_1, a_2, a_3, a_4\}$ $\qquad$ $B = \{b_1, b_2, b_3, b_4\}$



$(A, \leq)$

$(B, \leq')$

- $f(a_i) = b_i$ $(1 \leq i \leq 4)$ is order preserving.

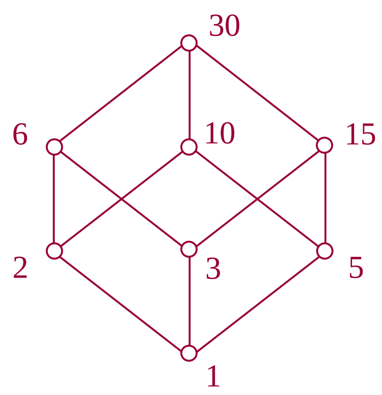
  $a_i \leq a_j \;\to\; f(a_i) = b_i \leq' b_j = f(a_j)$ for all i, j.

- $f^{-1}: B \to A$ is not order preserving.

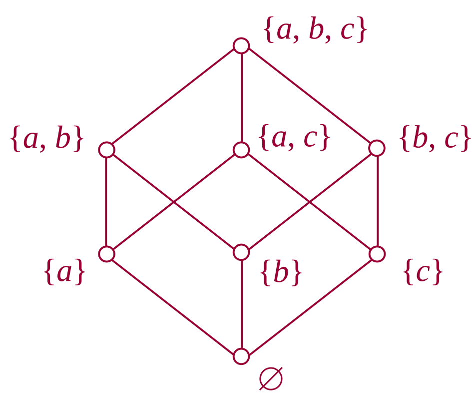
- Definition:

  Let $(A, \le)$ and $(B, \le')$ be two posets and let $f : A \to B$. If both f and f^{-1} is order preserving, then f is said to be an order isomorphism (or just isomorphism) between $(A, \le)$ and $(B, \le')$ and the posets are said to be order-isomorphic (or just isomorphic).

Example:



$\Leftrightarrow$

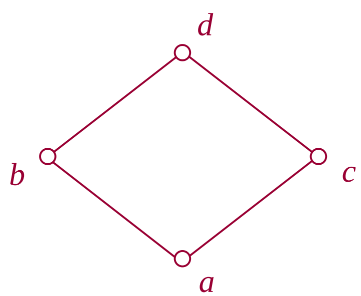


Lattices

- Definition:

  A poset $(A, \leq)$ is said to be a lattice if for every $a, b \in A$ there is an LUB and a GLB.

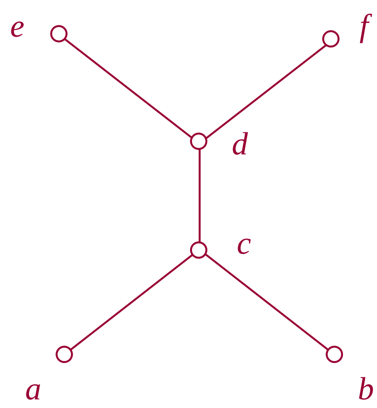
Examples:



Lattice

GLB$(b, c) = a$ LUB$(b, c) = d$

GLB$(a, b) = a$ LUB$(a, b) = b$



Not a lattice

Lattice

Not a lattice

(identity relation)

- Operation:
  - An n-ary operation on a set A is a function.

$$f : \underbrace{A \times A \times \cdots \times A}_{n} \to A$$

  - Binary operation:

$$f : A \times A \to A$$

  - On a lattice, GLB and LUB are binary operations.
    - GLB(a, b) = $a * b$
    - LUB(a, b) = $a + b$

- Theorem:

  If $(A, \leq)$ is a lattice, then for any $x, y \in A$

  1. $x * y = x$ iff $x \leq y$
  2. $x + y = y$ iff $x \leq y$

Proof of 1:

(if part)

Assume $x \leq y$.

Since $x \leq x$ and $x \leq y$, x is a lower bound of x and y.

We know $x * y$ is also a lower bound and it is the greatest lower bound.

Thus $x \leq x * y$.

Proof *of 1*:

But $x * y$ is a lower bound of x and y. Thus $x * y \leq x$.

From $x \leq x * y$ and $x * y \leq x$, we conclude that $x * y = x$.

(only if part)

Assume $x * y = x$.

We know $x * y$ is the greatest lower bound of x and y.

Thus $x * y \leq y$.

Since $x * y = x$, we conclude that $x \leq y$.

□

- Theorem:

  If $(A, \leq)$ is a lattice, then for every $x, y, z \in A$ the following are true:

  1. $x * x = x$ $\quad x + x = x$ idempotent laws
  2. $x * y = y * x$ $\quad x + y = y + x$ commutative laws
  3. $x * (y * z) = (x * y) * z$ $\quad x + (y + z) = (x + y) + z$ associative laws
  4. $x * (x + y) = x$ $\quad x + (x * y) = x$ absorption laws

Proof of 1:

Using the previous theorem and the fact that $x \leq x$, we can easily show that $x * x = x$ and $x + x = x$. □

Proof of 4: $x * (x + y) = x$

$x \leq x + y$ because $x + y$ is the least upper bound of x and y.

Again, using the previous theorem, $x * (x + y) = x$. □

- Lemma:

Let $(A, \leq)$ be a lattice. For every $x, y, z \in A$, if $y \leq z$ then $x * y \leq x * z$.

Proof :

Note that $x * z$ is the greatest lower bound of x and z.

All we need to show is that $x * y$ is a lower bound of x and z.

Obviously, $x * y \leq x$.

Since $x * y \leq y$ and $y \leq z$, we have $x * y \leq z$.

Therefore, $x * y$ is a lower bound of x and z. □

Proof of 3: $x * (y * z) = (x * y) * z$

First we want to prove that $x * (y * z) \leq (x * y) * z$.

Note that $(x * y) * z$ is the greatest lower bound of $x * y$ and z.

All we need to show is that $x * (y * z)$ is a lower bound of $x * y$ and z.

Since $y * z \leq y$, we get $x * (y * z) \leq x * y$ by the previous lemma.

From $x * (y * z) \leq y * z$ and $y * z \leq z$, we get $x * (y * z) \leq z$.

Therefore, $x * (y * z)$ is a lower bound of $x * y$ and z.

Now, we want to prove that $(x * y) * z \leq x * (y * z)$.

Notice that $(x * y) * z \leq x * y \leq x$.

Since $x * y \leq y$, we get $(x * y) * z \leq y * z$ by the previous lemma and the commutative law.

Proof of 3: $x * (y * z) = (x * y) * z$

Hence, $(x * y) * z$ is a lower bound of x and $y * z$.

But, $x * (y * z)$ is the greatest lower bound of x and $y * z$.

Therefore, $(x * y) * z \leq x * (y * z)$.

From $x * (y * z) \leq (x * y) * z$ and $(x * y) * z \leq x * (y * z)$,

we conclude that $x * (y * z) = (x * y) * z$. □

Algebra

$$\overset{\text{set}}{\downarrow}\!\!\!(A, \overbrace{\underbrace{O_{11}, O_{12}, \ldots, O_{1n_1}}_{\text{unary operations}}, \underbrace{O_{21}, O_{22}, \ldots, O_{2n_2}}_{\text{binary operations}}, \ldots, \underbrace{O_{k1}, O_{k2}, \ldots, O_{kn_k}}_{k\text{-ary operations}}}^{\text{operations on } A})$$

- **Theorem**:

  Let $(A, *, +)$ be an algebra such that the following four pairs of laws are satisfied:

  1. $x * x = x$ $\qquad$ $x + x = x$
  2. $x * y = y * x$ $\qquad$ $x + y = y + x$
  3. $x * (y * z) = (x * y) * z$ $\qquad$ $x + (y + z) = (x + y) + z$
  4. $x * (x + y) = x$ $\qquad$ $x + (x * y) = x$

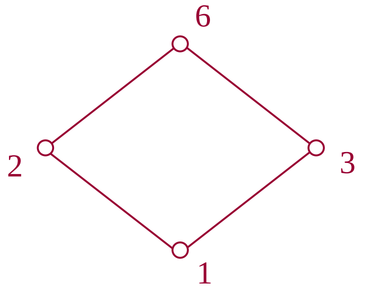
  Then $(A, \leq)$ is a lattice if $x \leq y$ when $x * y = x$ and/or $x + y = y$ for every $x, y \in A$.

Example:

- $A = \{1, 2, 3, 6\}$, $a * b = \mathrm{GCD}(a, b)$, $a + b = \mathrm{LCM}(a, b)$
  - $\mathrm{GCD}(a, a) = a$
  - $\mathrm{GCD}(a, b) = \mathrm{GCD}(b, a)$
  - $\mathrm{GCD}(a, \mathrm{GCD}(b, c)) = \mathrm{GCD}(\mathrm{GCD}(a, b), c)$
  - $\mathrm{GCD}(a, \mathrm{LCM}(a, b)) = a$
- $(a, b) \in R$ when $\mathrm{GCD}(a, b) = a$ and/or $\mathrm{LCM}(a, b) = b$.
  - $R = \{(1, 1), (1, 2), (1, 3), (1, 6), (2, 2), (2, 6), (3, 3), (3, 6), (6, 6)\}$

    R is a partial ordering.

    (A, R) is a lattice.



Proof:

First, we want to show that $\leq$ is a partial ordering.

Since $x * x = x$ for every $x \in A$ by 1, we have $x \leq x$ for every $x \in A$ and so $\leq$ is reflexive.

Let $x \leq y$ and $y \leq x$. Then $x * y = x$ and $y * x = y$.

But $x * y = y * x$ is given by 2, and so $x = y$.

Thus $\leq$ is antisymmetric.

Let $x \leq y$ and $y \leq z$. Then $x * y = x$ and $y * z = y$.

Substituting $y * z$ for y in $x * y = x$, we get $x * (y * z) = x$.

By applying 3, we get $(x * y) * z = x$.

Substituting x for $x * y$, we get $x * z = x$.

Thus $x \leq z$ and so $\leq$ is transitive.

Proof:

Since $\leq$ is reflexive, antisymmetric, and transitive, $\leq$ is a partial ordering.

Now we have to show that there exists a GLB and an LUB of x and y for every $x, y \in A$.

Since $x * (x + y) = x$ for every $x, y \in A$ by 4, we have $x \leq x + y$.

Similarly since $y * (y + x) = y$, we have $y \leq y + x = x + y$.

From $x \leq x + y$ and $y \leq x + y$, we conclude that $x + y$ is an upper bound of x and y.

If $x + y$ is the only upper bound, then it is the LUB of x and y.

If not, we need to show that $x + y$ is the least one among all the upper bounds of x and y.

Proof:

Suppose there is another upper bound, say z, of x and y.

In this case, $x \le z$ and $y \le z$, and thus $x + z = z$ and $y + z = z$.

Substituting $y + z$ for z in the left hand side of $x + z = z$, we get $x + (y + z) = z$.

Using 3, we get $(x + y) + z = z$.

Hence, $x + y \le z$ and thus $x + y$ is the LUB of x and y.

We can similarly show that $x * y$ is the GLB of x and y.

Therefore, $(A, \le)$ is a lattice.

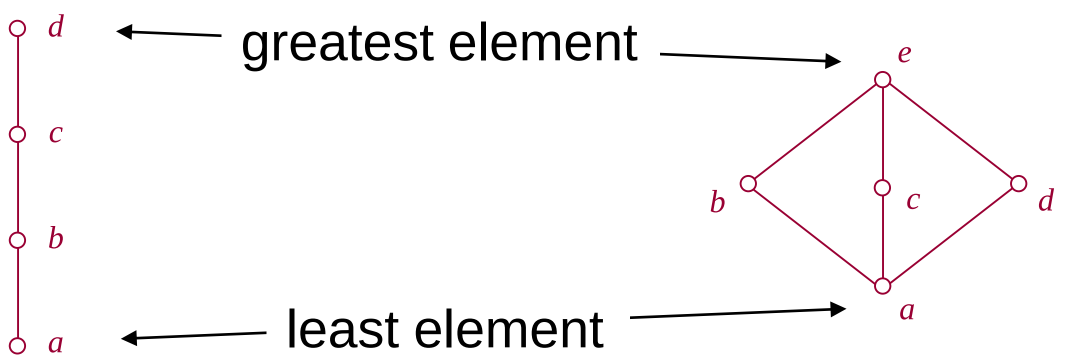
□

Boolean Lattice and Boolean Algebra

- Definition:

  A lattice $(A, \leq)$ is said to be a bounded lattice if the set A has a greatest element and a least element.

Example:

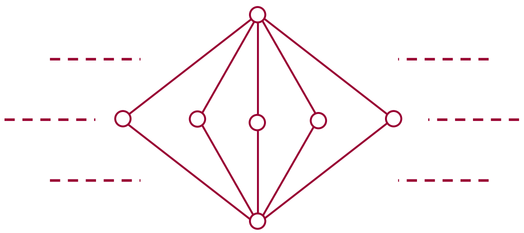


- Note:
  - In a bounded lattice $(A, \leq)$,
    - the greatest element is usually denoted by '1', and
    - the least element is usually denoted by '0'.

    For all $x \in A$,
    - $0 \leq x$ and thus $0 * x = 0$ and $0 + x = x$
    - $x \leq 1$ and thus $x + 1 = 1$ and $x * 1 = x$

- Theorem:

  If $(A, \leq)$ is a finite lattice then it is a bounded lattice.
  (The converse is not necessarily true.)

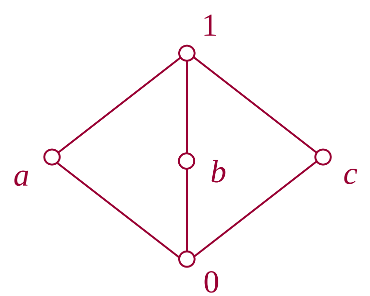


- Definition:

  A bounded lattice $(A, \leq)$ is said to be a complemented lattice if for every $x \in A$ there is an $\bar{x} \in A$ such that $x * \bar{x} = 0$ and $x + \bar{x} = 1$.

<u>Example</u>:

- Let x be a complement of a. Then,
  - $a * x = 0 \;\rightarrow\; x = b, c, 0$
  - $a + x = 1 \;\rightarrow\; x = b, c, 1$
  - ➡ $\bar{a} = b$ or $\bar{a} = c$

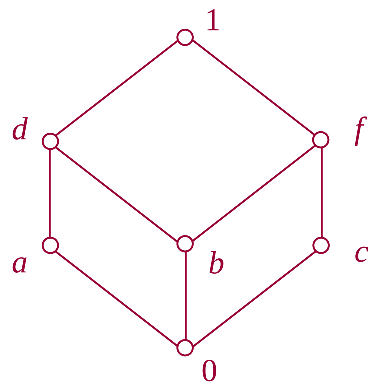


A complemented lattice

Example:

- $b * x = 0 \;\rightarrow\; x = a, c, 0$
- $b + x = 1 \;\rightarrow\; x = 1$

➡ There is no $\overline{b}$.



Not a complemented lattice

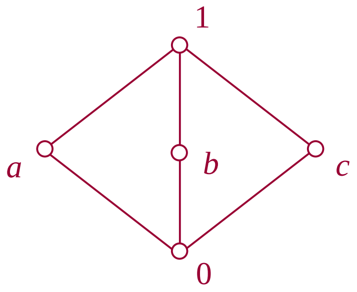
- **Definition**:

  A bounded lattice $(A, \leq)$ is said to be a distributive lattice if for every $x, y, z \in A$ the following are satisfied:

  1. $x * (y + z) = (x * y) + (x * z)$, and
  2. $x + (y * z) = (x + y) * (x + z)$

Example:

- $a * (b + c) = a * 1 = a$
- $(a * b) + (a * c) = 0 + 0 = 0$
- ➡ Not a distributive lattice



poset

↓

lattice

↓

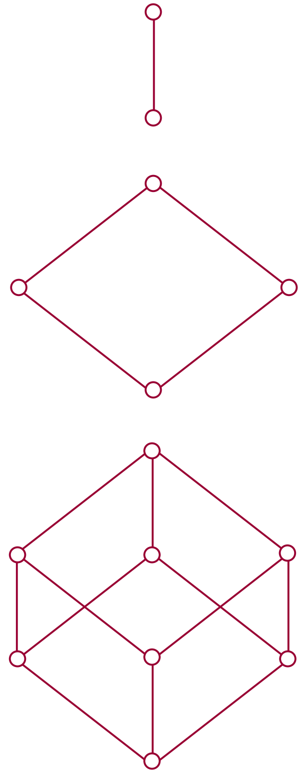
bounded lattice

↙ ↘

complemented lattice　　distributive lattice

↘ ↙

Boolean lattice



Boolean lattices

- Lattice and algebra:
  - From a lattice $(A, \leq)$ we can define an algebra $(A, *, +)$, and vice versa.

lattice $(A, \leq)$ $\cdots$ $(A, *, +)$ algebra

Boolean lattice $(A, \leq)$ $\cdots$ $(A, \underbrace{*, +}_{\text{binary operations}}, \underbrace{\overline{}}_{\text{unary operation}}, \underbrace{0, 1}_{\text{constants}})$ Boolean algebra

- Boolean algebra:
  - The following four laws are satisfied: (lattice)
    - idempotent law
    - commutative law
    - associative law
    - absorption law
  - $x + 0 = x$ and $x * 1 = x$ for every $x \in A$. (bounded lattice)
  - For every $x \in A$ there is $\bar{x} \in A$ such that $x * \bar{x} = 0$ and $x + \bar{x} = 1$. (complemented lattice)
  - For every $x, y, z \in A$ we have $x * (y + z) = (x * y) + (x * z)$ and $x + (y * z) = (x + y) * (x + z)$ (distributive lattice)