



COMP9020

Foundations of Computer Science

Lecture 8: Equivalence Relations and Partial Orders

Lecturers: Katie Clinch (LIC)
Paul Hunter
Simon Mackenzie

Course admin: Nicholas Tandiono

Course email: `cs9020@cse.unsw.edu.au`

Outline

Equivalence Relations

Partial Orders

Feedback

Outline

Equivalence Relations

Partial Orders

Feedback

Equivalence relations

Equivalence relations capture a general notion of “equality”. They are relations which are:

- Reflexive (R): Every object should be “equal” to itself
- Symmetric (S): If x is “equal” to y , then y should be “equal” to x
- Transitive (T): If x is “equal” to y and y is “equal” to z , then x should be “equal” to z .

Definition

A binary relation $R \subseteq S \times S$ is *equivalence relation* if it satisfies (R), (S), (T).

Example

Partition of \mathbb{Z} into classes of numbers with the same remainder on division by p ; it is particularly important for p prime

$$\mathbb{Z}(p) = \mathbb{Z}_p = \{0, 1, \dots, p-1\}$$

One can define all four arithmetic operations (with the usual properties) on \mathbb{Z}_p for a prime p ; division has to be restricted when p is not prime.

NB

$(\mathbb{Z}_p, +, \cdot, 0, 1)$ are fundamental algebraic structures known as **rings**. These structures are very important in coding theory and cryptography.

Equivalence Classes and Partitions

Suppose $R \subseteq S \times S$ is an equivalence relation

The **equivalence class** $[s]$ (w.r.t. R) of an element $s \in S$ is

$$[s] = \{t : t \in S \text{ and } sRt\}$$

Fact

$s R t$ if and only if $[s] = [t]$.

Equivalence classes: Proof example

Proof

Suppose $[s] = [t]$. Recall $[s] = \{x \in S : (s, x) \in R\}$. We will show that $(s, t) \in R$.

Because R is reflexive, $(t, t) \in R$.

Therefore $t \in [t]$.

Because $[t] = [s]$, it follows that $t \in [s]$.

But then $(s, t) \in R$ by the definition of $[s]$.

Equivalence classes: Proof example

Proof

Now suppose $(s, t) \in R$. We will show $[s] = [t]$ by showing $[s] \subseteq [t]$ and $[t] \subseteq [s]$.

Take any $x \in [s]$.

By the definition of $[s]$, $(s, x) \in R$.

Since R is symmetric $(x, s) \in R$.

Since R is transitive and $(s, t) \in R$ we have that $(x, t) \in R$.

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

Therefore, $x \in [t]$.

Therefore $[s] \subseteq [t]$.

Equivalence classes: Proof example

Proof

Now suppose $(s, t) \in R$. We will show $[s] = [t]$ by showing $[s] \subseteq [t]$ and $[t] \subseteq [s]$.

Take any $x \in [t]$.

By the definition of $[t]$, $(t, x) \in R$.

Since R is transitive and $(s, t) \in R$ we have that $(s, x) \in R$.

Therefore $x \in [s]$.

Therefore $[t] \subseteq [s]$.



Partitions

Definition

A **partition** of a set S is a collection of sets S_1, \dots, S_k such that

- S_i and S_j are disjoint (for $i \neq j$)
- $S = S_1 \cup S_2 \cup \dots \cup S_k = \bigcup_{i=1}^k S_i$

The collection of all equivalence classes $\{[s] : s \in S\}$ forms a partition of S .

In the opposite direction, a partition of a set defines the equivalence relation on that set. If $S = S_1 \cup \dots \cup S_k$, then we can define $\sim \subseteq S \times S$ as:

$s \sim t$ exactly when s and t belong to the same S_i .

Exercises

Exercises

RW: 3.6.6 (supp)

- (d) Show that $m \sim n$ iff $m^2 \equiv_{(5)} n^2$ is an equivalence on $S = \{1, \dots, 7\}$.

Find all the equivalence classes.

Outline

Equivalence Relations

Partial Orders

Feedback

Partial Order

A **partial order** \preceq on S satisfies (R), (AS), (T).

We call (S, \preceq) a **poset** — partially ordered set

Examples

Posets:

- (\mathbb{Z}, \leq)
- $(\text{Pow}(X), \subseteq)$ for some set X
- $(\mathbb{N}, |)$

Not posets:

- $(\mathbb{Z}, <)$
- $(\mathbb{Z}, |)$

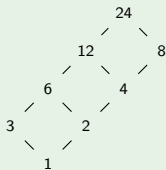
Hasse diagram

Every finite poset (S, \preceq) can be represented with a **Hasse diagram**:

- Nodes are elements of S
- An edge is drawn *upward* from x to y if $x \prec y$ and there is no z such that $x \prec z \prec y$

Example

Hasse diagram for positive divisors of 24 ordered by \mid :



Ordering Concepts

Definition

Let (S, \preceq) be a poset.

- **Minimal** element: x such that there is no $y \neq x$ with $y \preceq x$
- **Maximal** element: x such that there is no $y \neq x$ with $x \preceq y$
- **Minimum (least)** element: x such that $x \preceq y$ for all $y \in S$
- **Maximum (greatest)** element: x such that $y \preceq x$ for all $y \in S$

NB

- *There may be multiple minimal/maximal elements.*
- *Minimum/maximum elements are the unique minimal/maximal elements if they exist.*
- *Minimal/maximal elements always exist in finite posets, but not necessarily in infinite posets.*

Examples

Examples

- $\text{Pow}(\{a, b, c\})$ with the order \subseteq
 \emptyset is minimum; $\{a, b, c\}$ is maximum
- $\text{Pow}(\{a, b, c\}) \setminus \{\{a, b, c\}\}$ (proper subsets of $\{a, b, c\}$)
Each two-element subset $\{a, b\}, \{a, c\}, \{b, c\}$ is maximal.
 - But there is no maximum

Ordering Concepts

Definition

Let (S, \preceq) be a poset.

- x is an **upper bound** for A if $a \preceq x$ for all $a \in A$
- x is a **lower bound** for A if $x \preceq a$ for all $a \in A$
- The **set of upper bounds** for A is defined as
$$\text{ub}(A) = \{x : a \preceq x \text{ for all } a \in A\}$$
- The **set of lower bounds** for A is defined as
$$\text{lb}(A) = \{x : x \preceq a \text{ for all } a \in A\}$$
- The **least upper bound** of A , $\text{lub}(A)$, is the minimum of $\text{ub}(A)$ (if it exists)
- The **greatest lower bound** of A , $\text{glb}(A)$ is the maximum of $\text{lb}(A)$ (if it exists)

glb and lub

To show x is $\text{glb}(A)$ you need to show:

- x is a lower bound: $x \preceq a$ for all $a \in A$.
- x is the greatest of all lower bounds: If $y \preceq a$ for all $a \in A$ then $y \preceq x$.

Example

$\text{Pow}(X)$ ordered by \subseteq .

- $\text{glb}(A, B) = A \cap B$
- $\text{lub}(A, B) = A \cup B$

Ordering Concepts

Definition

Let (S, \preceq) be a poset.

- (S, \preceq) is a **lattice** if $\text{lub}(x, y)$ and $\text{glb}(x, y)$ exist for every pair of elements $x, y \in S$.
- (S, \preceq) is a **complete lattice** if $\text{lub}(A)$ and $\text{glb}(A)$ exist for every subset $A \subseteq S$.

NB

A finite lattice is always a complete lattice.

Examples

Examples

- $\{1, 2, 3, 4, 6, 8, 12, 24\}$ partially ordered by divisibility is a lattice
 - e.g. $\text{lub}(\{4, 6\}) = 12$; $\text{glb}(\{4, 6\}) = 2$
- $\{1, 2, 3\}$ partially ordered by divisibility is not a lattice
 - $\{2, 3\}$ has no lub
- $\{2, 3, 6\}$ partially ordered by divisibility
 - $\{2, 3\}$ has no glb
- $\{1, 2, 3, 12, 18, 36\}$ partially ordered by divisibility
 - $\{2, 3\}$ has no lub (12, 18 are minimal upper bounds)

NB

*An infinite lattice need not have a lub (or no glb) for an arbitrary infinite subset of its elements, in particular no such bound may exist for **all** its elements.*

Examples

- (\mathbb{Z}, \leq) : neither $\text{lub}(\mathbb{Z})$ nor $\text{glb}(\mathbb{Z})$ exist
- $(\mathcal{F}(\mathbb{N}), \subseteq)$ [all finite subsets of \mathbb{N}]: lub exists for pairs of elements but not generally for (infinite) sets of elements. glb exists for any set of elements: intersection of a set of finite sets is finite.
- $(\mathcal{I}(\mathbb{N}), \subseteq)$ [all infinite subsets of \mathbb{N}]: glb does not exist for some pairs of elements (e.g. odds and evens). lub exists for any set of elements: union of a set of infinite sets is always infinite.

Exercises

RW: 11.1.5 Consider poset (\mathbb{R}, \leq)

- (a) Is this a lattice?
- (b) Give an example of a non-empty subset of \mathbb{R} that has no upper bound.
- (c) Find $\text{lub}(\{x \in \mathbb{R} : x < 73\})$
- (d) Find $\text{lub}(\{x \in \mathbb{R} : x \leq 73\})$
- (e) Find $\text{lub}(\{x : x^2 < 73\})$
- (f) Find $\text{glb}(\{x : x^2 < 73\})$

Total orders

Definition

A **total order** is a partial order that also satisfies:

(L) *Linearity* (any two elements are comparable):

For all x, y either: $x \leq y$ or $y \leq x$ (or both if $x = y$)

NB

On a finite set all total orders are “isomorphic”

On an infinite set there is quite a variety of possibilities.

Examples

Examples

- \mathbb{Z} with \leq :
(no minimum/maximum element)
- \mathbb{Z} with
 $\{(x, y) : (xy \leq 0 \text{ and } x \leq y) \text{ or } (xy > 0 \text{ and } |x| \leq |y|)\}$:
(no maximum element, minimum element is -1)
- \mathbb{Z} with $\{(x, y) : (xy \leq 0 \text{ and } x \geq y) \text{ or } (xy > 0 \text{ and } x \leq y)\}$:
(minimum element 1, maximum element -1)

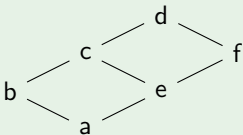
Ordering of a Poset — Topological Sort

Definition

For a poset (S, \preceq) any total order \leq that is consistent with \preceq (if $a \preceq b$ then $a \leq b$) is called a **topological sort**.

Example

Consider



The following all are topological sorts:

$$a \leq b \leq e \leq c \leq f \leq d$$

$$a \leq e \leq b \leq f \leq c \leq d$$

$$a \leq e \leq f \leq b \leq c \leq d$$

Well-Ordered Sets

Definition

A **well-ordered set** is a poset where every subset has a least element.

NB

The greatest element is not required.

Examples

- $\mathbb{N} = \{0, 1, \dots\}$
- Disjoint union of copies of \mathbb{N} :

$$\mathbb{N}_1 \dot{\cup} \mathbb{N}_2 \dot{\cup} \mathbb{N}_3 \dot{\cup} \dots,$$

where each $\mathbb{N}_i \simeq \mathbb{N}$ and $\mathbb{N}_1 < \mathbb{N}_2 < \mathbb{N}_3 \dots$

NB

Well-ordered sets are an important mathematical tool to prove termination of programs.

Orders for Cartesian products and languages

There are several practical ways of combining orders:

- **Product order:** Given posets (S, \preceq_S) and (T, \preceq_T) , define:

$$(s, t) \preceq (s', t') \quad \text{if } s \preceq_S s' \text{ and } t \preceq_T t'$$

Notes

- No implicit weighting.
- No bias toward any component.
- In general, it is only a partial order, even if combining total orders.

Orders for Cartesian products and languages

There are several practical ways of combining orders:

- **Product order:** Given posets (S, \preceq_S) and (T, \preceq_T) , define:

$$(s, t) \preceq (s', t') \quad \text{if } s \preceq_S s' \text{ and } t \preceq_T t'$$

- **Lexicographic order** Given posets (S, \preceq_S) and (T, \preceq_T) , define:

$$(s, t) \leq_{\text{lex}} (s', t') \quad \text{if } s \preceq_S s' \text{ or } (s = s' \text{ and } t \preceq_T t')$$

Notes

- No implicit weighting.
- Gives total order when combining total orders.
- Can be sensibly extended to words.

Orders for Cartesian products and languages

There are several practical ways of combining orders:

- **Product order:** Given posets (S, \preceq_S) and (T, \preceq_T) , define:

$$(s, t) \preceq (s', t') \quad \text{if } s \preceq_S s' \text{ and } t \preceq_T t'$$

- **Lexicographic order** Given posets (S, \preceq_S) and (T, \preceq_T) , define:

$$(s, t) \leq_{\text{lex}} (s', t') \quad \text{if } s \preceq_S s' \text{ or } (s = s' \text{ and } t \preceq_T t')$$

Extension to words: $\lambda \leq_{\text{lex}} w$ for all words

Notes

- No implicit weighting.
- Gives total order when combining total orders.
- Can be sensibly extended to words.
- Not ideal for enumeration.

Orders for Cartesian products and languages

There are several practical ways of combining orders:

- **Product order:** Given posets (S, \preceq_S) and (T, \preceq_T) , define:

$$(s, t) \preceq (s', t') \quad \text{if } s \preceq_S s' \text{ and } t \preceq_T t'$$

- **Lexicographic order** Given posets (S, \preceq_S) and (T, \preceq_T) , define:

$$(s, t) \leq_{\text{lex}} (s', t') \quad \text{if } s \preceq_S s' \text{ or } (s = s' \text{ and } t \preceq_T t')$$

Extension to words: $\lambda \leq_{\text{lex}} w$ for all words

- **Lenlex order:** Lexicographic ordering, but order by length first.

Notes

- Only applicable for languages (subsets of Σ^*).
- Gives total order when Σ is totally ordered.
- Gives an enumeration of Σ^* .

Example

Example

RW: 11.2.5 Let $\mathbb{B} = \{0, 1\}$ with the usual order $0 < 1$. List the elements 101, 010, 11, 000, 10, 0010, 1000 of \mathbb{B}^* in the

(a) Lexicographic order

(b) Lenlex order

RW: 11.2.8 When are the lexicographic order and *lenlex* on Σ^* the same?

Exercises

RW: 11.6.6 True or false?

- (a) If a set Σ is totally ordered, then the corresponding lexicographic partial order on Σ^* also must be totally ordered.
- (b) If a set Σ is totally ordered, then the corresponding lenlex order on Σ^* also must be totally ordered.
- (c) Every finite poset has a Hasse diagram.
- (d) Every finite poset has a topological sorting.
- (e) Every finite poset has a minimum element.
- (f) Every finite totally ordered set has a maximum element.
- (g) An infinite poset cannot have a maximum element.

Outline

Equivalence Relations

Partial Orders

Feedback

Weekly Feedback

We would appreciate any comments/suggestions/requests you have on this week's lectures.



<https://forms.office.com/r/aHRCGANHiB>