Lecture 12

Axiom of Choice, Cardinality, Cantor's theorem

MATH 411H, FALL 2025

October 13, 2025

Partially ordered sets

Partial ordering

A **partial ordering** on a nonempty set X is a relation R on X with the following properties:

(a) xRx for all $x \in X$, (reflexivity).

(b) If xRy and yRx, then $x = y$, (antisymmetry).

(c) If xRy and yRz, then xRz, (transitivity).

Linear ordering

If R additionally satisfies that for all $x, y \in X$ either xRy or yRx, then R is called **linear** or **total ordering** on X.

Example

The set of rational numbers $\mathbb{Q}$ with the natural order $\leq$ is totally ordered set. We say that $r \leq s$ for $r, s \in \mathbb{Q}$ iff $s - r \geq 0$.

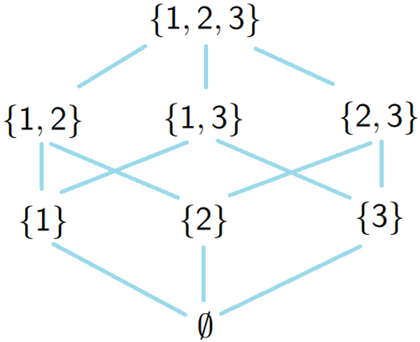
Examples of partial ordering

Example

If X is any set then $\mathcal{P}(X)$ is partially ordered by inclusion, i.e.

$$ARB \iff A \subseteq B.$$

Consider $X = \{1, 2, 3\}$ and we have its Hasse diagram



Poset $\equiv$ partially ordered set

Poset

We say that $(X, \leq)$ is a **poset** if the relation "$\leq$" is a partial ordering on X or $(X, \leq)$ is partially ordered by "$\leq$".

- We will write $x < y$ in a poset $(X, \leq)$ iff $x \leq y$ and $x \neq y$.

Upper (lower) bound

Let $A \subseteq X$, an element $x \in X$ is an **upper bound** of A (resp. **lower bound** of A) if $a \leq x$ for all $a \in A$ (resp. $x \leq a$ for all $a \in A$).

- **An upper (lower) bound $x \in X$ need not to belong to A.**

Maximal and greatest elements

Maximal (minimal) element

A **maximal** (resp. **minimal**) element of X is an element $x \in X$ such that if $y \in X$ and $x \leq y$ (resp. $x \geq y$) then $x = y$.

Greatest (least) element

A **greatest** (resp. **least**) element of X is an element $x \in X$ such that $y \leq x$ for all $y \in X$ (resp. $x \leq y$ for all $y \in X$).

Well ordered set

If $(X, \leq)$ is linearly ordered and every non-empty subset of X has a minimal element, which is necessarily unique, X is said to be well ordered by $\leq$ and $\leq$ is called **well ordering** on X.

Examples

- $(\mathbb{N}, \leq)$ is well ordered in contrast to $(\mathbb{Z}, \leq)$ which is not well ordered.

Supremum and infimum of A

Supremum of A

Let $A \subseteq X$ be bounded above. We say that an element $x_0 \in X$ is **the least upper bound for** A or **the supremum of** A ($x_0 = \sup A$) if the following hold:

1. $a \leq x_0$ for all $a \in A$,
2. if $a \leq x$ for all $a \in A$, then $x_0 \leq x$.

Infimum of A

Let $A \subseteq X$ be bounded below. We say that an element $x_0 \in X$ is **the greatest lower bound for** A or **the infimum of** A ($x_0 = \inf A$) if the following hold:

1. $x_0 \leq a$ for all $a \in A$,
2. if $x \leq a$ for all $a \in A$, then $x \leq x_0$.

Four equivalent statements

Theorem (The axiom of choice (A))

If $(X_\alpha)_{\alpha\in A}$ is a nonempty collection of nonempty sets, then $\prod_{\alpha\in A} X_\alpha \neq \emptyset$.

Theorem (The Hausdorff Maximal Principle (B))

Every partially ordered set has a maximal linearly ordered set, i.e. if $(X, \leq)$ is a poset there exists $E \subseteq X$ that is linearly ordered by $\leq$ such that no subset of X that properly includes E is linearly ordered by $\leq$.

Theorem (Kuratowski–Zorn lemma (C))

If X is partially ordered set and every linearly ordered subset of X has an upper bound, then X has a maximal element.

Theorem (The Well Ordering Principle (D))

Every nonempty set X can be well ordered.

An auxiliary result

Theorem

Let $(X, \leq)$ be a poset such that every linearly ordered subset of X has a supremum in X. Then every function $f : X \to X$ obeying

$$x \leq f(x) \quad \textit{for all} \quad x \in X$$

has a fixed point, i.e. there is $x^* \in X$ such that $f(x^*) = x^*$.

Proof. Clearly the empty set $\emptyset$ is linearly ordered so it has the supremum in X, i.e. $a = \sup \emptyset \in X$, which is the smallest element in $(X, \leq)$.

Let $\mathcal{A} \subseteq \mathcal{P}(X)$ be the family of all $A \subseteq X$ such that

- (a) $a \in A$,
- (b) $f[A] \subseteq A$,
- (c) if $L \subseteq A$ is linearly ordered set in $(X, \leq)$, then $\sup L \in A$.

Proof

- Note that $\mathcal{A} \neq \emptyset$ since $X \in \mathcal{A}$. Then consider

$$A_* = \bigcap_{A \in \mathcal{A}} A.$$

- It is easy to see that $A_* \in \mathcal{A}$, equivalently A_* satisfies (a), (b), (c).

$$f[A_*] = f\left[\bigcap_{A \in \mathcal{A}} A\right] \subseteq \bigcap_{A \in \mathcal{A}} f[A] \subseteq \bigcap_{A \in \mathcal{A}} A = A_*.$$

- Our aim will be to prove that A_* is linearly ordered set in $(X, \leq)$.
- Consider

$$B = \{x \in A_* : \text{ if } y \in A_* \text{ and } y < x \text{ then } f(y) \leq x\}.$$

- We shall show that $B \in \mathcal{A}$.

Proof

- **Proof of (a) for B.** Observe that $a \in B$ since $a \in A_*$ and a is the smallest element of $(X, \leq)$, so there is no element y such that $y < a$. Thus, $a \in B$, hence (a) holds for B.
- Fix $x \in B$ and define

$$B_x = \{z \in A_* \ : \ z \leq x \text{ or } f(x) \leq z\} \subseteq A_*$$

- We will show that $B_x \in \mathcal{A}$ for all $x \in B$.
- **Proof of (a) for B_x.** Note that $a \in B_x$ since $a \leq x$ for all $x \in X$.
- **Proof of (b) for B_x.** Take $z \in B_x$ and we show that $f(z) \in B_x$. It will ensure that $f[B_x] \subseteq B_x$. Since $z \in B_x$ so $z \leq x$ or $f(x) \leq z$.
- If $z < x$ then $f(z) \leq x$ by definition of B, so $f(z) \in B_x$.
- Otherwise $x = z$ or $f(x) \leq z$. If $x = z$ then $f(z) = f(x)$ so $f(z) \in B_x$. If $f(x) \leq z$, then

$$f(x) \leq z \leq f(z)$$

  thus we also have $f(z) \in B_x$.

Proof

- **Proof of (c) for B_x.** Let $L \subseteq B_x$ be a linearly ordered set. We will show that $\sup L \in B_x$.
- If all elements $z \in L$ satisfy $z \leq x$, then $\sup L \leq x$ and consequently $\sup L \in B_x$.
- If $f(x) \leq z$ for some $z \in L$, then

  $$f(x) \leq z \leq \sup L,$$

  then $\sup L \in B_x$.
- Thus we have proved that $B_x \in \mathcal{A}$ for all $x \in B$ since

  $$A_* = \bigcap_{A \in \mathcal{A}} A \subseteq B_x \subseteq A_*$$

  so $B_x = A_*$ for all $x \in B$. This means that

  $$z \leq x \quad \text{or} \quad f(x) \leq z \quad \text{for all} \quad x \in B \quad \text{and} \quad z \in A_*. \qquad (*)$$

Proof

- **Proof of (b) for B.** Let $x \in B$. We will show that $f(x) \in B$. Recall

$$B = \{x \in A_* : \text{ if } y \in A_* \text{ and } y < x \text{ then } f(y) \leq x\} \subseteq A_*.$$

- Let $y \in A_*$ be such that $y < f(x)$. Then by (*) we have $y \leq x$. If $y < x$ then by the definition of B we have

$$f(y) \leq x \leq f(x),$$

  so $f(x) \in B$. If $x = y$ then $f(x) = f(y)$ and also $f(x) \in B$.
- **Proof of (c) for B.** Let $L \subseteq B$ be a linearly ordered set in B. We will show that $\sup L \in B$. Let $y \in A_*$ be so that $y < \sup L$, then there is $x \in L$ such that $x \not\leq y$. By (*) we have $y < x$. By the definition of B one obtains $f(y) \leq x$. Since $x \in L$ then $f(y) \leq x \leq \sup L$ thus $\sup L \in B$ as desired.

Proof

- We have proved that $B \in \mathcal{A}$, hence

$$A_* = \bigcap_{A \in \mathcal{A}} A \subseteq B \subseteq A_*,$$

thus $B = A_*$.

- Hence, by (*) for all $x, z \in A_* = B$ we have $z \leq x$ or $f(x) \leq z$. So

$$x \leq z \quad \text{or } z \leq x.$$

- Now it is easy to see that $x_* = \sup A_* \in A_*$ by (c). Moreover, x_* is a fixed point of f. Since by (b) we have

$$x_* \leq \underbrace{f(x_*)}_{\in A_*} \leq x_* = \sup A_*.$$

Thus $x_* = f(x_*)$ as claimed. □

Auxiliary result

Theorem

If $(X, \leq)$ is a poset such that every linearly ordered set has a supremum, then X contains a maximal element.

Proof. Suppose for a contradiction that there is no maximal element in X. So for every $x \in X$ there is $y \in X$ such that $x < y$. In other words, the sets

$$A_x = \{y \in X : x < y\} \neq \emptyset.$$

Thus $\prod_{x \in X} A_x \neq \emptyset$ by the axiom of choice. Now take $f \in \prod_{x \in X} A_x$, then $f(x) \in A_x$, so $x < f(x)$. By the previous theorem $x \leq f(x)$ for all $x \in X$, hence there is $x_* \in X$ such that $x_* < f(x_*) = x_*$, contradiction! □

Theorem

The principles (A), (B), (C), and (D) are equivalent.

Proof (A) $\implies$ (B)

Proof (A) $\implies$ (B).

- Principle (B) says that if $(X, \leq)$ is a poset then X has a maximal linearly ordered set.
- Let $\mathcal{L}$ be a set of all linearly ordered subsets in $(X, \leq)$. Note that $(\mathcal{L}, \subseteq)$ is a poset ordered by inclusion $\subseteq$.
- Let $\mathcal{M} \subseteq \mathcal{L}$ be a linearly ordered set. It is easy to see that

$$\mathcal{S} = \bigcup_{M \in \mathcal{M}} M$$

  is a linearly ordered set in $(X, \leq)$ and $\mathcal{S}$ is the supremum for $\mathcal{M}$.
- Thus from the previous theorem there exists a maximal element $L \in \mathcal{L}$ which is the maximal linearly ordered set in $(X, \leq)$. $\square$

Proof (B) $\implies$ (C)

Proof (B) $\implies$ (C).

- Principle (C) states that if $(X, \leq)$ is a poset and every linearly ordered subset of X has an upper bound, then X has maximal element.
- By (B) there is a maximal linearly ordered set $L \subseteq X$. From the assumption in (C) the set L has an upper bound in X.
- Let $a \in X$ be the upper bound for L. From maximality of L in X we must have that $a \in L$, or else $L \cup \{a\}$ contradicts the maximality of L.
- Then a is a maximal element of X. If we take $x \in X \setminus L$ such that $a \leq x$, then $a = x$. Otherwise we consider $L \cup \{x\}$ which is linearly ordered set containing L, and this contradicts the maximality of L. $\square$

Proof (C) $\implies$ (D)

Proof (C) $\implies$ (D).

- Principle (D) states that every nonempty set X can be well ordered. Let $\mathcal{W}$ be the collection of well-orderings of subsets of X defined by

$$\mathcal{W} = \{(E, \leq) : E \subseteq X \text{ and } \leq \text{ is well ordering on } E\}$$

  and define the partial ordering on $\mathcal{W}$ as follows: If the relations $\leq_1$ and $\leq_2$ are well orderings on E_1 and E_2 respectively, then $\leq_1$ precedes $\leq_2$ in the partial order if:

  1. $\leq_2$ extends $\leq_1$, i.e. $E_1 \subseteq E_2$ and $\leq_1$ and $\leq_2$ agree on E_1.
  2. if $x \in E_2 \setminus E_1$, then $y \leq_2 x$ for all $y \in E_1$.

- It is easy to see that the hypotheses of (C) are satisfied on $\mathcal{W}$. We take $\mathcal{L} \subseteq \mathcal{W}$ to be a linearly ordered set in $\mathcal{W}$ and we note that $\bigcup_{L \in \mathcal{L}} L$ is an upper bound for $\mathcal{L}$. Then (C) implies that there is a maximal element $(E, \leq) \in \mathcal{W}$.

Proof (C) $\implies$ (D) and (D) $\implies$ (A)

- This must be a well ordering on X itself. If $\leq$ is a well ordering on a proper subset $E \subset X$ and $x_0 \in X \setminus E$ then $\leq$ can be extended to a well ordering on $E \cup \{x_0\}$ by declaring that $x \leq x_0$ for all $x \in E$, but this is a contradiction since $(E, \leq)$ is a maximal element of $\mathcal{W}$. □

Proof (D) $\implies$ (A).

- Suppose that $(X_\alpha)_{\alpha \in A}$ is a nonempty collection of nonempty sets. Let

$$X = \bigcup_{\alpha \in A} X_\alpha.$$

- Using (D) we pick a well ordering on X. For any $\alpha \in A$ let $f(\alpha)$ be the minimal element of X_α. Then

$$f \in \prod_{\alpha \in A} X_\alpha \neq \emptyset. \qquad \square$$

Cardinality

Cardinality

If X and Y are nonempty sets, we define the expressions

$$\mathrm{card}\,(X) \leq \mathrm{card}\,(Y) \quad \text{(injective)},$$

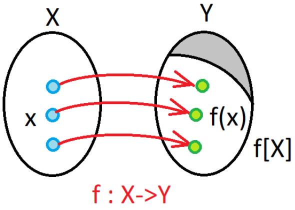
$$\mathrm{card}\,(X) = \mathrm{card}\,(Y) \quad \text{(bijective)},$$

$$\mathrm{card}\,(X) \geq \mathrm{card}\,(Y) \quad \text{(surjective)},$$

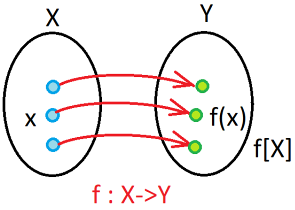
to mean that there exists $f : X \to Y$ which is injective, bijective, surjective respectively.

Cardinality - pictures 1/2

$\mathrm{card}\,(X) \leq \mathrm{card}\,(Y)$, (injective),

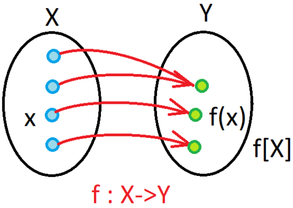


$\mathrm{card}\,(X) = \mathrm{card}\,(Y)$, (bijective)



Cardinality - pictures 2/2

$\text{card}\,(X) \geq \text{card}\,(Y)$, (surjective)



- We also define $\text{card}\,(X) < \text{card}\,(Y)$ to mean that there is an injection but not a bijection.
- We also have $\text{card}\,(\emptyset) < \text{card}\,(X)$ and $\text{card}\,(X) > \text{card}\,(\emptyset)$ for all $X \neq \emptyset$.

$\mathrm{card}\,(X)$ -example

Example

Let

$$X = \{1, 2, 3, 4, \dots\}$$

$$Y = \{101, 102, 103, \dots, \}.$$

Prove that $\mathrm{card}\,(X) = \mathrm{card}\,(Y)$.

Solution. Let us define $f : X \to Y$ by

$$f(x) = x + 100,$$

then f is a bijection between X and Y, so $\mathrm{card}\,(X) = \mathrm{card}\,(Y)$. □

card (X) - example

Example

Let

$$X = \{1, 2, 3, 4, \ldots\}$$

$$Y = \{1^2, 2^2, 3^2, 4^2, \ldots, \}.$$

Prove that card $(X) = $ card (Y).

Solution 1. Let us define $f : X \to Y$ by

$$f(x) = x^2,$$

then f is a bijection between X and Y, so card $(X) = $ card (Y). $\square$

Solution 2. Let us define $g : Y \to X$ by

$$f(x) = \sqrt{x},$$

then g is a bijection between X and Y, so card $(X) = $ card (Y). $\square$

$\mathrm{card}\,(X)$ - example

Example

Let

$$X = \{1, 2, 3\}$$

$$Y = \{2, 4, 6, 8\}.$$

Prove that $\mathrm{card}\,(X) < \mathrm{card}\,(Y)$.

Solution. Note that $f(x) = 2x$ is an injection from X to Y, so $\mathrm{card}\,(X) \leq \mathrm{card}\,(Y)$. On the other hand, any function from X to Y takes at most 3 values, so it is not a surjection, so $\mathrm{card}\,(X) < \mathrm{card}\,(Y)$. □

$\mathrm{card}\,(X)$ - example

Example

Let

$$X = [0, 1]$$
$$Y = [1, 3].$$

Prove that $\mathrm{card}\,(X) = \mathrm{card}\,(Y)$.

Solution. Let us define $f : X \to Y$ by

$$f(x) = 2x + 1,$$

then f is a bijection between X and Y, so $\mathrm{card}\,(X) = \mathrm{card}\,(Y)$. □

Proposition

Proposition

We have

$$\mathrm{card}\,(X) \leq \mathrm{card}\,(Y) \iff \mathrm{card}\,(Y) \geq \mathrm{card}\,(X).$$

Proof (⇒). Assume that $\mathrm{card}\,(X) \leq \mathrm{card}\,(Y)$. This means that there is an injection $f : X \to Y$. Thus f is a bijection $f : X \to f[X] \subseteq Y$. Let f^{-1} be the inverse $f^{-1} : f[X] \to X$. Pick $x_0 \in X$ and define g by

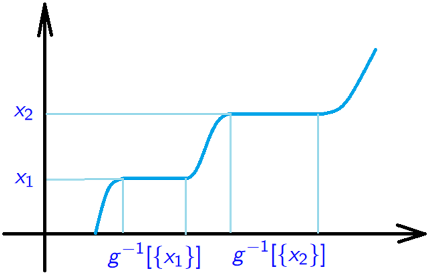
$$g(y) = \begin{cases} f^{-1}(y) \text{ if } y \in f[X], \\ g(y) = x_0 \text{ if } y \in Y \setminus f[X]. \end{cases}$$

Then we see that g is surjective from Y to X.

Proof: 1/2

Proof (⇐). If $\mathrm{card}\,(Y) \geq \mathrm{card}\,(X)$, then there is a surjection $g : Y \to X$. Then $g[Y] = X$, and, consequently, $g^{-1}[\{x\}]$ are nonempty and

$$g^{-1}[\{x_1\}] \cap g^{-1}[\{x_2\}] = \emptyset \quad \text{if} \quad x_1 \neq x_2.$$



Proof: 2/2

Using the axiom of choice the set $\prod_{x\in X} g^{-1}[\{x\}] \neq \emptyset$. Taking

$$f \in \prod_{x\in X} g^{-1}[\{x\}]$$

we see that f is an injection from X to Y. Indeed, if $x_1 \neq x_2$, then $f(x_1) \in g^{-1}[\{x_1\}]$ and $f(x_2) \in g^{-1}[\{x_2\}]$, but

$$g^{-1}[\{x_1\}] \cap g^{-1}[\{x_2\}] = \emptyset,$$

thus $f(x_1) \neq f(x_2)$. □