Module 2: Set Theory

Operational math bootcamp

Statistical Sciences
UNIVERSITY OF TORONTO

Huanlin Mao

University of Toronto

July 9, 2025

Outline

- Review of basic set theory
- Ordered Sets
- Functions

Introduction to Set Theory

- We define a *set* to be a collection of mathematical objects.
- If S is a set and x is one of the objects in the set, we say x is an element of S and denote it by $x \in S$.

$S = \{1, 2, 3\}$, $2 \in S$, $5 \notin S$

- The set of no elements is called empty set and is denoted by $\emptyset$.

Fact: ϕ is a subset of any set

$P \Rightarrow Q$

If P is false, the implication is always true

To show $S=T$, we need to show

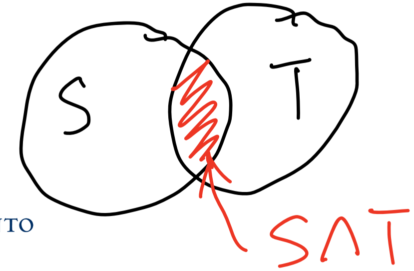
1) $s \in S$ implies $s \in T$ 2) $s \in T$ implies $s \in S$.

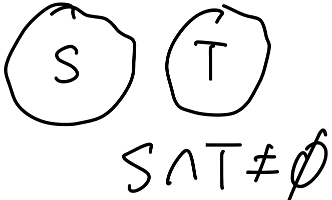
Definition (Subsets, Union, Intersection)

Let S, T be sets.

$S \subseteq T \iff \forall s, s \in S \Rightarrow s \in T$

- We say that S is a *subset* of T, denoted $S \subseteq T$, if $s \in S$ implies $s \in T$.
- We say that $S = T$ if $S \subseteq T$ and $T \subseteq S$.
- We define the *union* of S and T, denoted $S \cup T$, as all the elements that are in *either* S or T. inclusive or
- We define the *intersection* of S and T, denoted $S \cap T$, as all the elements that are in *both* S and T.
- We say that S and T are *disjoint* if $S \cap T = \emptyset$.





Some examples

natural number

integers

real number

Example

$\mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

$\mathbb{N}_0 = N \cup \{0\}$

rational number

complex

Example

Let $a, b \in \mathbb{R}$ such that $a < b$.

Open interval: $(a, b) := \{x \in \mathbb{R} : a < x < b\}$ (a, b may be $-\infty$ or $+\infty$)

Closed interval: $[a, b] := \{x \in \mathbb{R} : a \leq x \leq b\}$

We can also define half-open intervals.

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

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

Example

Let $A = \{x \in \mathbb{N} : 3|x\}$ and $B = \{x \in \mathbb{N} : 6|x\}$ Show that $B \subseteq A$.

Proof. To prove $B \subseteq A$, we need to show $\forall x \in B$, we have $x \in A$

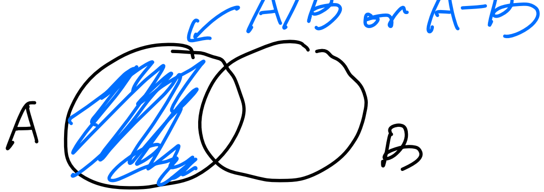
Let x be any/arbitrary element in B,

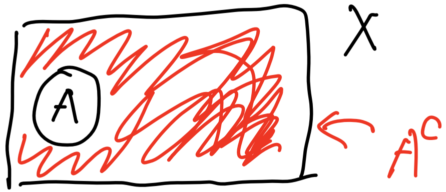
By definition of B, $\exists k \in \mathbb{N}$, s.t. $x = 6 \cdot k$

Then, $x = 6 \cdot k = 3(\underbrace{2k}_{\in \mathbb{N}}) \in A$ by definition of A

So we have $B \subseteq A$

Difference of sets





Definition

Let $A, B \subseteq X$. We define the *set-theoretic difference* of A and B, denoted $A \setminus B$ (sometimes $A - B$) as the elements of X that are in A but *not* in B.
The complement of a set $A \subseteq X$ is the set $A^c := X \setminus A$.

complement relative ~~to~~ which large set?

Example

Let $X \subseteq \mathbb{R}$ be defined as $X = \{x \in \mathbb{R} : 0 < x \leq 40\} = (0, 40]$. Then

$X^c = (-\infty, 0] \cup (40, \infty)$

Recall that for sets S, T:

- the *union* of S and T, denoted $S \cup T$, is all the elements that are in *either* S and T
- and the *intersection* of S and T, denoted $S \cap T$, is all the elements that are in *both* S and T.

We extend the definition of union and intersection to an arbitrary family of sets as follows:

Definition

Let S_α, $\alpha \in A$, be a family of sets. A is called the *index set*. We define

$$\bigcup_{\alpha \in A} S_\alpha := \{x : \exists \alpha \text{ such that } x \in S_\alpha\},$$

x is in the union if x is in at least one of the sets

$$\bigcap_{\alpha \in A} S_\alpha := \{x : x \in S_\alpha \text{ for all } \alpha \in A\}.$$

x is in the intersection if x is in every one of the sets

$\forall x \in \mathbb{R}$, we can chose an integer n

s.t. $|x| \leq n$,

Then $x \in [-n, n]$

Therefore $\bigcup_{n=1}^{\infty} [-n, n] \supseteq \mathbb{R}$

Example

$$\bigcup_{n=1}^{\infty} [-n, n] = \mathbb{R}$$

$\bigcup_{n=1}^{\infty} [-n, n] \subseteq \mathbb{R}$

$$\bigcap_{n=1}^{\infty} \left(-\frac{1}{n}, \frac{1}{n}\right) = \{0\}$$

1) clearly, $0 \in (-\frac{1}{n}, \frac{1}{n})$

2) if $x \neq 0$, we can an integer n

s.t. $1/n < |x|$

$x \notin (-\frac{1}{n}, \frac{1}{n})$

$x \notin \bigcap_{n=1}^{\infty} (-\frac{1}{n}, \frac{1}{n})$

Theorem (De Morgan's Laws)

Let $\{S_\alpha\}_{\alpha\in A}$ be an arbitrary collection of sets. Then

$$\left(\bigcup_{\alpha\in A} S_\alpha\right)^c = \bigcap_{\alpha\in A} S_\alpha^c \quad \textit{and} \quad \left(\bigcap_{\alpha\in A} S_\alpha\right)^c = \bigcup_{\alpha\in A} S_\alpha^c$$

Proof.

$$\bigcup_{\alpha\in A} S_\alpha = \{x \mid \exists \alpha \in A \text{ s.t. } x \in S_\alpha\}$$

negate

$$\left(\bigcup_{\alpha\in A} S_\alpha\right)^c = \{x \mid \forall \alpha \in A, \underbrace{x \notin S_\alpha}_{x\in S_\alpha^c}\} = \{x \mid \forall \alpha\in A, x \in S_\alpha^c\}$$

$$= \bigcap_{\alpha\in A} S_\alpha^c$$

by definition

– intersection

To prove the second one, $\left(\bigcap_{\alpha\in A} S_\alpha\right)^c = \bigcup_{\alpha\in A} S_\alpha^c$

we can reduce it to the first one.

By the first result

$$\left(\bigcup_{\alpha\in A} S_\alpha^c\right)^c = \bigcap_{\alpha\in A} (S_\alpha^c)^c = \bigcap_{\alpha\in A} S_\alpha$$

Taking complement of both sides, we have

$$\bigcup_{\alpha\in A} S_\alpha^c = \left(\bigcap_{\alpha\in A} S_\alpha\right)^c.$$

of

Since a set is itself a mathematical object, a set can itself contain sets.

Definition

The power set $\mathcal{P}(S)$ of a set S is the set of all subsets of S.

Example

Let $S = \{a, b, c\}$.
Then $\mathcal{P}(S) = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}\}$

$|P(S)| = 8 = 2^3 = 2^{|S|}$

$|P(S)| = 2^{|S|}$ $\rightarrow$ holds for any set with finite $|S|$

Another way of building a new set from two old ones is the Cartesian product of two sets.

Definition

Let S, T be sets. The *Cartesian product* $S \times T$ is defined as the set of tuples with elements from S, T, i.e

$$S \times T = \{(s, t) : s \in S \text{ and } t \in T\}.$$

This can also be extended inductively to a finite family of sets.

Ex. $S = T = \mathbb{R}$, $S \times T = \mathbb{R}^2$

$(x, y) \in \mathbb{R} \times \mathbb{R}$, $x, y \in \mathbb{R}$

Ordered set

$2 \leq 3$ is a example of relation.

Definition

A relation R on a set X is a subset of $X \times X$. A relation $\leq$ is called a *partial order* on X if it satisfies

1. reflexivity: $x \leq x$ i.e. $(x, x) \in R \subseteq X \times X$
2. transitivity: if $x \leq y$, $y \leq z$, then we have $x \leq z$ i.e. $(x,y) \in R$, $(y,z) \in R$, then $(x,z) \in R \subseteq X \times X$
3. anti-symmetry: if $x \leq y$, $y \leq x$, then $x = y$ i.e. $(x,y) \in R$, $(y,x) \in R$, then $x = y$

The pair $(X, \leq)$ is called a *partially ordered set*.

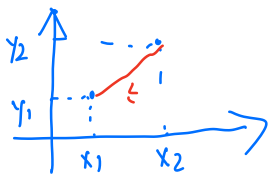
if $x \neq y$, we can not have

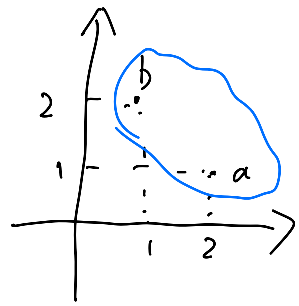
A *chain* or *totally ordered set* $C \subseteq X$ is a subset with the property $x \leq y$ or $y \leq x$ for any $x, y \in C$.

$(x,y) \in R$ and $(y,x) \in R$ at same time.

$\mathbb{R}$, $\mathbb{R} \times \mathbb{R}$ or $\mathbb{R}^2$

Define relation by $(x_1, y_1) \le (x_2, y_2) \overset{def}{\iff} x_1 \le x_2$ and $y_1 \le y_2$





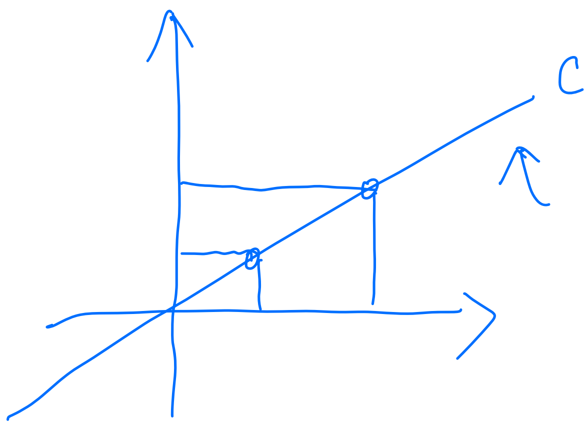
$a = (2, 1) \in \mathbb{R}^2$

$b = (1, 2) \in \mathbb{R}^2$

No order between A and B

$\mathbb{R}^2$ is not totally order.

$\exists\, x, y \in \mathbb{R}^2$, we do not have $(x, y) \in R \subseteq \mathbb{R}^2 \times \mathbb{R}^2$



C is totally ordered subset / chain

$(\mathbb{R}^2, \underset{\uparrow}{\leq})$, are not totally ordered.

$1 \leq 2 \leq 3$ we've defined above

Example

The real numbers with the usual ordering, $(\mathbb{R}, \leq)$ are totally ordered.

Example

The power set of a set X with the ordering given by $\subseteq$, $(\mathcal{P}(X), \subseteq)$ is a partially ordered set.

E.g. $X = \{1, 2, 3\}$. Then $P(X) = \{\phi, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

$\phi \subseteq \{1\}$. $\{1\} \subseteq \{1,2\} \subseteq \{1,2,3\}$

But, $\{1,2\}$ $\{1,3\}$ do not have order

Example

Let $X = \{a, b, c, d\}$. What is $\mathcal{P}(X)$? Find a chain in $\mathcal{P}(X)$.

$\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{b, c\}, \{c, d\}, \{b, d\}, \{a, c\}, \{a, d\}, \{a, b, c\}, \{b, c, d\}, \{a, b, d\}, \{a, c, d\}, X\}$

$\{\phi, \{a\}\} \subseteq \mathcal{P}(X)$, $\phi \subsetneq \{a\}$

$\phi \subseteq \{a\} \subseteq \{a, b\} \subseteq \{a, b, c\} \subseteq X$

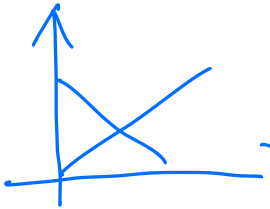
Example

Consider the set $C([0,1],\mathbb{R}) := \{f : [0,1] \to \mathbb{R} : f \text{ is continuous}\}$.

For two functions $f, g \in C([0,1],\mathbb{R})$, we define the ordering as $f \leq g$ if $f(x) \leq g(x)$ for $x \in [0,1]$. Then $(C([0,1],\mathbb{R}), \leq)$ is a partially ordered set.

Can you think of a chain that is a subset of $(C([0,1],\mathbb{R})$?

A. It is not a totally ordered set.



$f(x) = x$

$g(x) = 1 - x$

no order

E.g. ① constant function

② fix $f_0(x)$,

$\{f_n(x) \mid f_n(x) = f_0(x) + n,\ n \in \mathbb{R}\}$

③ .....

Definition

A non-empty partially ordered set $(X, \leq)$ is *well-ordered* if every non-empty subset $A \subseteq X$ has a mimimum element.

$\exists\, a \in A, \quad \forall\, b \in A, \quad a \leq b$, or $(a, b) \in R \subseteq X \times X$

Example:

$(\mathbb{N}, \leq)$ is... well-ordered

$(\mathbb{R}, \leq)$ is... not well-ordered.

$\mathbb{R}$ itself

(a, b)

don't have minimum

assume $a < b$

Definition

Let $(X, \leq)$ be a partially ordered set and $S \subseteq X$.

Then $x \in X$ is an *upper bound* for S if for all $s \in S$ we have $s \leq x$.
Similarly, $y \in X$ is a *lower bound* for S if for all $s \in S$, $y \leq s$.

If there exists an upper bound for S, we call S *bounded above* and if there exists a lower bound for S, we call S *bounded below*. If S is bounded above and bounded below, we say S is *bounded*.

$S \subseteq X$, we may have lots of / infinte upper bound and lower bound.

$X = \mathbb{R}$, $S = [0, 1]$, 2 , 3 , 4 , $x \geq 1$, x is a upper bound

We can also ask if there exists a least upper bound or a greatest lower bound.

Definition

Let $(X, \leq)$ be a partially ordered set and $S \subseteq X$.

We call $x \in X$ *least upper bound* or *supremum*, denoted $x = \sup S$, if x is an upper bound and for any other upper bound $y \in X$ of S we have $x \leq y$.

1 2

Likewise, $x \in X$ is the *greatest lower bound* or *infimum* for S, denoted $x = \inf S$, if it is a lower bound and for any other lower bound $y \in X$, $y \leq x$.

1 2

Note that the supremum and infimum of a bounded set do not necessarily need to exist. However, if they do exists they are unique, which justifies the article *the* (exercise). Nevertheless, the reals have a remarkable property, which we will take as an axiom.

Completeness Axiom

Let $S \subseteq \mathbb{R}$ be bounded above. Then there exists $r \in \mathbb{R}$ such that $r = \sup S$, i.e. S has a least upper bound.

By setting $S' = -S := \{-s : s \in S\}$ and noting $\inf S = -\sup S'$, we obtain a similar statement for infima if S is bounded below. As mentioned above, this property is fairly special, for example it fails for the rationals.

$\mathbb{Q}$

Example

$\forall x \in S, \ x^2 < 9, \ -3 \le x \le 3$

Let $S = \{q \in \mathbb{Q} : x^2 < 7\}$. Then S is bounded above in $\mathbb{Q}$, but there exists no least upper bound in $\mathbb{Q}$.

$\sup S = \sqrt{7}$ is a irrational numbe

$\sup S \notin \mathbb{Q}$

If we consider sup and inf in $\mathbb{R}$, they do exist

There is a nice alternative characterization for suprema in the real numbers.

Proposition

Let $S \subseteq \mathbb{R}$ be bounded above. Then $r = \sup S$ if and only if r is an upper bound and for all $\epsilon > 0$ there exists an $s \in S$ such that $r - \epsilon < s$. $r < s + \varepsilon$

①

②

Proof. $(\Rightarrow)$ only if part

Suppose we have $r = \sup S$, prove it by contradiction

Suppose r is an upper bound, $\exists\ \varepsilon > 0,\ \forall s \in S,\ r - \varepsilon \geq s$

$r - \varepsilon$ is an upper bound of S

However, $r - \varepsilon < \underbrace{\sup S}_{r}$. This is a contradiction.

Proof. ($\Leftarrow$) if part. prove it by contradition.

Suppose. r is an upper bound of S. And $\forall \varepsilon > 0, \exists s \in S$, s.t. $r - \varepsilon < s$. (*)

Suppose $r \neq \sup S$. Since r is an upper bound. $r \geq \sup S$.

Next, let $\varepsilon = r - \sup S$. If $\varepsilon = 0$, $r = \sup S$ contradics.

If $\varepsilon > 0$, By (*), $r - \varepsilon < s$. Then $s > r - \varepsilon = r - (r - \sup S) = \sup S$.

$s > \sup S$ contradics.

Using the same trick, we may obtain a similar result for infima.

Example

Consider $S = \{1/n : n \in \mathbb{N}\}$. Then $\sup S = 1$ and $\inf S = 0$.

Functions

Definition

A function f from a set X to a set Y is a subset of $X \times Y$ with the properties:

1. For every $x \in X$, there exists a $y \in Y$ such that $(x, y) \in f \subseteq X \times Y$
2. If $(x, y) \in f$ and $(x, z) \in f$, then $y = z$. → For each x, only a unique y is associated.

X is called the *domain* of f.

How does this connect to other descriptions of functions you may have seen?

Example

For a set X, the identity function is:

$$1_X : X \to X, \quad x \mapsto x$$

Statistical Sciences
UNIVERSITY OF TORONTO

Definition (Image and pre-image)

Let $f: X \to Y$ and $A \subseteq X$ and $B \subseteq Y$.

- ~~The *image* of~~ f is the set $f(A) := \{f(x) : x \in A\}$. The image of A under f
- ~~The *pre-image* of~~ f is the set $f^{-1}(B) := \{x : f(x) \in B\}$. The pre-image of B under f

Helpful way to think about it for proofs:

Image: If $y \in f(A)$, then $y \in Y$, and there exists an $x \in A$ such that $y = f(x)$.

Pre-image: If $x \in f^{-1}(B)$, then $x \in X$ and $f(x) \in B$.

$(x, y) \in f \subseteq X \times Y$

Definition (Surjective, injective and bijective)

Let $f: X \to Y$, where X and Y are sets. Then

- f is *injective* if $x_1 \neq x_2$ implies $f(x_1) \neq f(x_2)$
- f is *surjective* if for every $y \in Y$, there exists an $x \in X$ such that $y = f(x)$
- f is *bijective* if it is both injective and surjective

or $(x,y) \in f \in X \times Y$

Example

Let $f: X \to Y$, $x \mapsto x^2$.

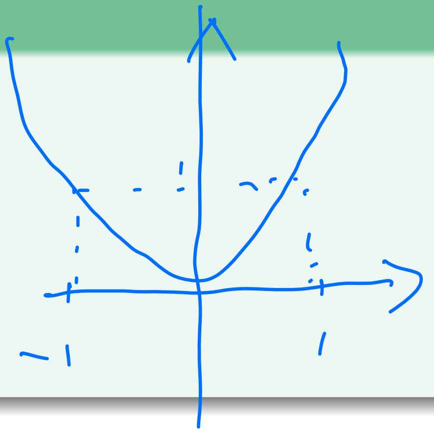
f is surjective if $X = \mathbb{R}$, $Y = \mathbb{R}_{\geq 0}$

f is injective if $X = \mathbb{R}_{\geq 0}$, $Y = \mathbb{R}$

f is bijective if $X = Y = \mathbb{R}_{\geq 0}$

f is neither surjective nor injective if

$X = Y = \mathbb{R}$



References

Marcoux, Laurent W. (2019). *PMATH 351 Notes*. url:
https://www.math.uwaterloo.ca/ lwmarcou/notes/pmath351.pdf

Runde ,Volker (2005). *A Taste of Topology*. Universitext. url:
https://link.springer.com/book/10.1007/0-387-28387-0

Zwiernik, Piotr (2022). *Lecture notes in Mathematics for Economics and Statistics*.
url: http://84.89.132.1/ piotr/docs/RealAnalysisNotes.pdf