Module 2: Set Theory

Operational math bootcamp

Statistical Sciences
UNIVERSITY OF TORONTO

Emma Kroell

University of Toronto

July 13, 2022

Outline

- Review of basic set theory
- Ordered Sets
- Functions
- Cardinality

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

Definition (Subsets, Union, Intersection)

Let S, T be sets.

- 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.
- 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

Example

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

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.

Example

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

Proof.

Let $x \in B$. Then $6|x$, so $\exists k \in \mathbb{Z}$ s.t. $x = 6k$.

Then $x = 3(2k)$ so $3|x$.

Thus $x \in A$.

$\square$

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 $A^c := X \setminus A$.

Example

Let $X \subseteq \mathbb{R}$ be defined as $X = \{x \in \mathbb{R} : 0 < x \leq 40\} = (0, 40]$. Then
$X^c = \{x \in \mathbb{R} : x \leq 0 \text{ or } x > 40\} = (-\infty, 0] \cup (40, \infty)$.

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

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

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

Example

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

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

Theorem (De Morgan's Laws)

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

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

1

Proof.

1 Let $x \in \left(\bigcup_{\alpha\in A} S_\alpha\right)^c$. This is true if and only if

$x \notin \bigcup_{\alpha\in A} S_\alpha \iff x \in S_\alpha^c \;\; \forall \alpha \in A$

$\iff x \in \bigcap_{\alpha\in A} S_\alpha^c$

Proof of 2 : exercise

□

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

2^n

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.

Ordered set

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: $x \leq x \quad \forall x \in X$
2. transitivity: $x, y, z \in X$, $x \leq y$ & $y \leq z \Rightarrow x \leq z$
3. anti-symmetry: $x, y \in X$, then $x \leq y$ and $y \leq x \Rightarrow x = y$

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

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

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 subsets, $(\mathcal{P}(X), \subseteq)$ is partially ordered set.

Example

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

Example

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

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

$$C = \{\emptyset, \{a\}, \{a, b\}, \{a, b, c\}, X\}$$

Statistical Sciences
UNIVERSITY OF TORONTO

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 $(C([0,1],\mathbb{R})$?

Definition

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

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 $\cancel{x}\, s \leq \cancel{s}\, x$. 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*.

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 $x \leq y$. 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 $y \in X$, $y \leq x$.

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.

Example

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 $\mathbb{Q}$.

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 $r - \epsilon < s$.

Proof.

($\Rightarrow$) We prove the contrapositive.

Suppose r is either not an upper bound or $\exists\, \varepsilon > 0$ s.t. $\forall s \in S$, $r - \varepsilon \geq s$.

In the first case, r cannot be the sup, $r \neq \sup S$.

In the second case, $r - \varepsilon$ is an upper bound for S and $r - \varepsilon < r$, so $r \neq \sup S$.

$\square$

Proof.

($\Leftarrow$) By contradiction.

Suppose r is an upper bound for S and $\forall \varepsilon > 0$ $\exists s \in S$ s.t. $r - \varepsilon < s$ but $r \neq \sup S$.

$\Rightarrow r > \sup S \iff r - \sup S > 0$

Then by assumption (in blue), $\exists s \in S$ s.t.

$r - (r - \sup S) = \sup S < s$. $\Rightarrow \Leftarrow$. $\therefore r = \sup S$

$\square$

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 $(x, y) \in f$
2. If $(x, y) \in f$ and $(x, z) \in f$, then $y = z$.

X is called the *domain* of f.

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

$f : X \to Y$ $\quad$ $x \mapsto y$ where $(x, y) \in f$

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

Helpful way to think about it for proofs:
If $y \in f(A)$, then $y \in Y$, and there exists an $x \in A$ such that $y = f(x)$.
If $x \in f^{-1}(B)$, then $x \in X$ and $f(x) \in B$.

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 bijective

Example

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

f is surjective if $X = \mathbb{R}$, $Y = [0, \infty)$

f is injective if $X = [0, \infty)$ $Y = \mathbb{R}$

f is bijective if $X = [0, \infty) = Y$

f is neither surjective nor injective if $Y = X = \mathbb{R}$

Proposition

Let $f : X \to Y$ and $A \subseteq X$. Prove that $A \subseteq f^{-1}(f(A))$, with equality iff f is injective.

if f is injective, $A = f^{-1}(f(A))$

Proof.

First, we show $A \subseteq f^{-1}(f(A))$. Let $x \in A$.
Let $B = f(A)$. $B \subseteq Y$. By definition, $f(x) \in B$.
Again using the definition, $x \in f^{-1}(B)$.
$\therefore x \in f^{-1}(f(A))$.

Now suppose f is injective. We want to show $f^{-1}(f(A)) \subseteq A$. Let $x \in f^{-1}(f(A))$. By def, $f(x) \in f(A)$. By definition, $\exists \tilde{x} \in A$ s.t. $f(x) = f(\tilde{x})$. Since f is injective, $x = \tilde{x}$.
$\therefore x \in A$.

$\square$

Cardinality

Intuitively, the *cardinality* of a set A, denoted $|A|$, is the number of elements in the set. For sets with only a finite number of elements, this intuition is correct. We call a set with finitely many elements finite.

We say that the empty set has cardinality 0 and is finite.

Proposition

(*) *If X is finite set of cardinality n, then the cardinality of $\mathcal{P}(X)$ is 2^n.*

Proof.

We prove this by induction on n. (Note: could also prove without using induction).

<u>Base case</u>: $n=0$ (i.e. $X=\emptyset$).

Then $\mathcal{P}(X)=\{\emptyset\}$, so $\mathcal{P}(X)$ has cardinality $1=2^0$. The statement holds for $n=0$.

Inductive hypothesis: suppose the statement (*) holds for some $n \in \mathbb{N}_0$.

□

Proof.

continued. Let X have $n+1$ elements. Let's call them $\{x_1, x_2, \ldots, x_n, x_{n+1}\}$. We can split X into 2 subsets $A = \{x_1, x_2, \ldots, x_n\}$ and $B = \{x_{n+1}\}$.

By the inductive hypothesis, $\mathcal{P}(A)$ has cardinality 2^n.

Any subset of X must either be a subset of A or contain x_{n+1}. We count the ones of the latter form. We take elements of A and combine with x_{n+1}.

nC_1

Count them: $1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n}$

$$= \sum_{k=0}^{n} \binom{n}{k} = 2^n$$

References

Therefore, the total number of elements in $\mathcal{P}(X)$ is $2^n + 2^n = 2^{n+1}$.

Thus the claim holds by induction.

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