Module 2: Set Theory

Operational math bootcamp

Statistical Sciences
UNIVERSITY OF TORONTO

Emma Kroell

University of Toronto

July 12, 2022

Outline

- Review of basic set theory
- Ordered Sets
- Functions
- Cardinality
- The Axiom of Choice

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.

$\square$

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

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

$$\bigcap_{\alpha \in A} S_\alpha := \{x : x \in S_\alpha \forall \alpha \in A\}$$

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*

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

Proof.

$\square$

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 $\mathcal{P}(S) =$

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

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

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: $x \leq x$ for all $x \in X$
2. transitivity: for $x, y, z \in X$, $x \leq y$ and $y \leq z$ implies $x \leq z$
3. anti-symmetry: for $x, y \in X$, $x \leq y$ and $y \leq x$ implies $x = y$

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

Consider the set $C([0,1],\mathbb{R}) := f : [0,1] \to \mathbb{R} : f$ is continuous.
For two function $f, g \in C([0,1],\mathbb{R})$, 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 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?

Example

For a set X, the identity function is:

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

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 $f(A) := \{f(x) : x \in A\}$ and 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

f is injective if

f is bijective if

f is neither surjective nor injective if

Proposition

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

Proof.

$\square$

Cardinality

Definition

The *cardinality* of a set A, denoted $|A|$, is the number of elements in the set.

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.

$\square$

Definition

Two sets A and B have same cardinality, $|A| = |B|$, if there exists bijection $f : A \to B$.

Example

Which is bigger, $\mathbb{N}$ or $\mathbb{N}_0$?

Cantor-Schröder-Bernstein

Definition

We say that the cardinality of a set A is less than the cardinality of a set B, denoted $|A| \leq |B|$ if there exists an injection $f : A \to B$.

Theorem (Cantor-Bernstein)

Let A, B, be sets. If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

Example

$|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$

Proof.

$\square$

Definition

Let A be a set.

1. A is *finite* if there exists an $n \in \mathbb{N}$ and a bijection $f : \{1, \ldots, n\} \to A$
2. A is *countably infinite* if there exists a bijection $f : \mathbb{N} \to A$
3. A is *countable* if it is finite or countably infinite
4. A is *uncountable* otherwise

Example

The rational numbers are countable, and in fact $|\mathbb{Q}| = |\mathbb{N}|$.

Let's look at $\mathbb{Q}^+ := \{x \in \mathbb{Q} : x > 0\}$. The fact that the rationals are countable relies on this famous way of listing the rational numbers:

$$\begin{array}{cccccc} 1 & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \cdots \\ 2 & \color{red}{\frac{2}{2}} & \frac{2}{3} & \color{red}{\frac{2}{4}} & \frac{2}{5} & \cdots \\ 3 & \frac{3}{2} & \color{red}{\frac{3}{3}} & \frac{3}{4} & \frac{3}{5} & \cdots \\ 4 & \color{red}{\frac{4}{2}} & \frac{4}{3} & \color{red}{\frac{4}{4}} & \frac{4}{5} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Example

This is a map from $\mathbb{N}$ to $\mathbb{Q}^+$. As long as we skip any fraction that is already in our list as we go along, it is injective. Since we can find an injection from $\mathbb{Q}^+$ to $\mathbb{N} \times \mathbb{N}$ (exercise), we have that $|\mathbb{Q}^+| = |\mathbb{N}|$. We can extend this to $\mathbb{Q}$. To do so, let $f : \mathbb{N} \to \mathbb{Q}^+$ be a bijection (which exists by the previous part). Then we can define another bijection $g : \mathbb{N} \to \mathbb{Q}$ by setting $g(1) = 0$ and

$$g(n) = \begin{cases} f(n) & \text{if } n \text{ is even,} \\ -f(n) & \text{if } n \text{ is odd,} \end{cases}$$

for $n > 1$.

Theorem

The cardinality of $\mathbb{N}$ is smaller than that of $(0,1)$.

Proof.

First, we show that there is an injective map from $\mathbb{N}$ to $(0,1)$.

Next, we show that there is no surjective map from $\mathbb{N}$ to $(0, 1)$. We use the fact that every number $r \in (0,1)$ has a binary expansion of the form $r = 0.\sigma_1\sigma_2\sigma_3\ldots$ where $\sigma_i \in \{0,1\}$, $i \in \mathbb{N}$. □

Proof.

Now we suppose in order to derive a contradiction that there does exist a surjective map f from $\mathbb{N}$ to (0, 1)., i.e. for $n \in \mathbb{N}$ we have $f(n) = 0.\sigma_1(n)\sigma_2(n)\sigma_3(n)\dots$. This means we can list out the binary expansions, for example like

$$
\begin{aligned}
f(1) =& 0.\color{red}{0}\color{black}{0000000}\dots \\
f(2) =& 0.1\color{red}{1}\color{black}{11111111}\dots \\
f(3) =& 0.01\color{red}{0}\color{black}{1010101}\dots \\
f(4) =& 0.101\color{red}{0}\color{black}{101010}\dots
\end{aligned}
$$

We will construct a number $\tilde{r} \in (0, 1)$ that is not in the image of f. □

Statistical Sciences
UNIVERSITY OF TORONTO

Proof.

Define $\tilde{r} = 0.\tilde{\sigma}_1\tilde{\sigma}_2\ldots$, where we define the nth entry of $\tilde{r}$ to be the the opposite of the nth entry of the nth item in our list:

$$\tilde{\sigma}_n = \begin{cases} 1 & \text{if } \sigma_n(n) = 0, \\ 0 & \text{if } \sigma_n(n) = 1. \end{cases}$$

Then $\tilde{r}$ differs from $f(n)$ at least in the nth digit of its binary expansion for all $n \in \mathbb{N}$. Hence, $\tilde{r} \notin f(\mathbb{N})$, which is a contradiction to f being surjective. This technique is often referred to as Cantor's diagonal argument. $\square$

Proposition

(0,1) and $\mathbb{R}$ have the same cardinality.

Proof.

The map $f : \mathbb{R} \to (0,1)$ defined by $x \mapsto \frac{1}{\pi}\left(\arctan(x) + \frac{\pi}{2}\right)$ is a bijection. $\square$

We have shown that there are different sizes of infinity, as the cardinality of $\mathbb{N}$ is infinite but still smaller than that of $\mathbb{R}$ or $(0,1)$. In fact, we have

$$|\mathbb{N}| = |\mathbb{N}_0| = |\mathbb{Z}| = |\mathbb{Q}| < |\mathbb{R}|.$$

Because of this, there are special symbols for these two cardinalities: The cardinality of $\mathbb{N}$ is denoted $\aleph_0$, while the cardinality of $\mathbb{R}$ is denoted $\mathfrak{c}$. There is even a relationship between them: $\mathfrak{c} = 2^{\aleph_0}$, i.e. the cardinality of $\mathbb{R}$ is the same as the cardinality of $\mathcal{P}(\mathbb{N})$.

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