Module 3: Set theory and metrics

Operational math bootcamp

Statistical Sciences
UNIVERSITY OF TORONTO

Ichiro Hashimoto

University of Toronto

July 10, 2024

Outline

- More on set theory
- Cardinality of sets
- Metrics and norms

Recall

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 $f^{-1}(B) := \{x : f(x) \in B\}$.

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

Proposition

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

Proof. First we prove $A \subset f^{-1}(f(A))$

Let $a \in A$. We need to show $a \in f^{-1}(f(A))$.

We need to show, $f(a) \in f(A)$.

This is trivial since $a \in A$,

(if part) Suppose f is injective.

Since we already know $A \subset f^{-1}(f(A))$, it suffices to show

$f^{-1}(f(A)) \subset A$.

Let $a \in f^{-1}(f(A))$.

Then $f(a) \in f(A)$.

Therefore, $\exists\, a' \in A$ s.t. $f(a) = f(a')$.

Since f is injective, $f(a) = f(a')$ implies $a = a' \in A$.

Thus, if part is completed.

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.

$X = \{x_1, \dots, x_n\}$. Let $A \subset X$

For each x_i $\to$ $\in A$ / $\notin A$ 2 options.

There are n elements in X.

So in total there are 2^n distinct subsets of X. $//$

$|A|$

Definition

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

injection + surjection

Example

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

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

A. $|\mathbb{N}| = |\mathbb{N}_0|$

Let $f : \mathbb{N} \to \mathbb{N}_0$ be $f(n) = n - 1$.

Then f is both injection and surjection.

Therefore, f is bijection. //

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 $f\colon A \to B$.

Theorem (Cantor-Bernstein)

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

$\exists$ injection $f: A \to B$ $\exists$ injection $g: B \to A$ $\exists$ bijection $h: A \to B$

Example

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

Proof that $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$:

Let $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ be $f(n) = (n, 1)$.

Then $n \neq m$ implies $f(n) = (n, 1) \neq (m, 1) = f(m)$

So, f is injective.

Let $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$g(n, m) = 2^n 3^m$

If $g(n, m) = g(n', m')$, then $2^n 3^m = 2^{n'} 3^{m'}$.

Then counting the exponent of primes 2, 3, we have $n = n'$, $m = m'$

thus g is injective.

Definition

Let A be a set.

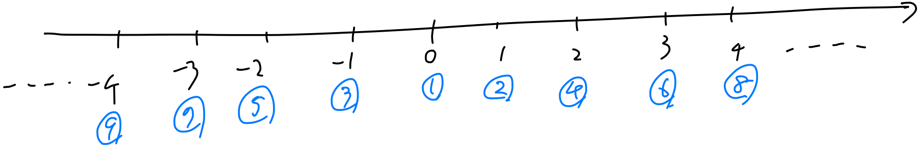
1. A is *finite* if there exists an $n \in \mathbb{N}$ and a bijection $f \colon \{1, \ldots, n\} \to A$
2. A is *countably infinite* if there exists a bijection $f \colon \mathbb{N} \to A$
3. A is *countable* if it is finite or countably infinite
4. A is *uncountable* otherwise

Example

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

Proof. ~~First we show~~ $\cancel{|\mathbb{N}| \le |\mathbb{Q}|}$.

We first show $|\mathbb{N}| = |\mathbb{Z}|$.



~~Next, we show that $|\mathbb{Q}^+| \leq |\mathbb{N} \times \mathbb{N}|$.~~

Next we show $|\mathbb{Q}| = |\mathbb{Z}|$.

Let $f: \mathbb{Z} \to \mathbb{Q}$ be $f(z) = z$. Then f is clearly injection.

Only thing left is construct injection $g: \mathbb{Q} \to \mathbb{Z}$.

For any $r \in \mathbb{Q}$, we can write $\frac{2}{3} = \cancel{\frac{4}{6}}$

$r = \frac{p}{q}$ when $p \in \mathbb{Z}$, $q \in \mathbb{N}$, p and q are mutually prime.

$$
\begin{array}{cccccc}
1^{1} & \frac{1}{2}^{2} & \frac{1}{3}^{4} & \frac{1}{4}^{6} & \frac{1}{5}^{10} & \cdots \\
2^{3} & \cancel{\frac{2}{2}} & \frac{2}{3}^{7} & \cancel{\frac{2}{4}} & \frac{2}{5} & \cdots \\
3^{5} & \frac{3}{2}^{8} & \cancel{\frac{3}{3}} & \frac{3}{4} & \frac{3}{5} & \cdots \\
4^{9} & \cancel{\frac{4}{2}} & \frac{4}{3} & \cancel{\frac{4}{4}} & \frac{4}{5} & \cdots \\
5^{11} & & & & & \\
\vdots & & & & &
\end{array}
$$

We can extend this to $\mathbb{Q}$ as follows:

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 $(0, 1)$.

Let $f : \mathbb{N} \to (0,1)$ be $f(n) = \frac{1}{n+1}$

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 $f(n) = 0.\sigma_1(n)\sigma_2(n)\sigma_3(n)\ldots$. This means we can list out the binary expansions, for example like

$$
\begin{aligned}
f(1) &= 0.\underbrace{0}_{=\sigma_1(1)}0000000\ldots \\
f(2) &= 0.1\underbrace{1}_{=\sigma_2(2)}11111111\ldots \\
f(3) &= 0.01\underbrace{0}1010101\ldots \\
f(4) &= 0.101\underbrace{0}_{=\sigma_4(4)}101010\ldots
\end{aligned}
$$

diagonal entries

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

find $\tilde{r} \notin f(\mathbb{N})$

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:

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

$\Rightarrow$ $\tilde{\sigma}_n \neq \sigma_n(n)$ for any n.

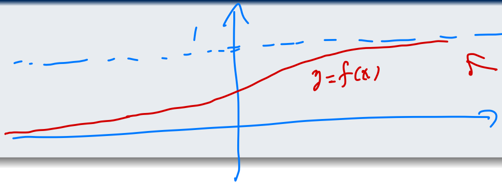
$\Rightarrow$ $\tilde{r} \neq f(n)$ for any n.

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.



monotone, continuous. $0 < f(x) < 1$

$\lim_{x \to \infty} f(x) = 1$, $\lim_{x \to -\infty} f(x) = 0$

$\square$

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 $\mathfrak{c}$.
In fact there are many other cardinalities, as the following theorem shows:

Theorem (Cantor's theorem)

For any set A, $|A| < |\mathcal{P}(A)|$.

Metric Spaces

distance between two points.

Definition (Metric)

A *metric* on a set X is a function $d : X \times X \to \mathbb{R}$ that satisfies:

(a) Positive definiteness: $d(x,y) \geq 0$ for $\forall x,y$. and $d(x,y)=0$ iff $x=y$

(b) Symmetry: $d(x,y) = d(y,x)$

(c) Triangle inequality: $d(x,y) + d(y,z) \geq d(x,z)$

A set together with a metric is called a metric space.

Example ($\mathbb{R}^n$ with the Euclidean distance)

$$d(x,y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}. \quad , \forall x,y \in \mathbb{R}^n.$$

On $\mathbb{R}^1$, $\quad d(x,y) = |x-y|.$

$\mathbb{R}, \mathbb{C}$

Definition (Norm)

A *norm* on an $\mathbb{F}$-vector space E is a function $\|\cdot\| : E \to \mathbb{R}$ that satisfies:

(a) Positive definiteness: $\|x\| \geq 0 \quad \forall x \in E$ and $\|x\| = 0$ iff $x = 0$

(b) Homogeneity: For $\forall x \in E$, $\forall \alpha \in \mathbb{F}$, $\|\alpha x\| = |\alpha| \, \|x\|$.

(c) Triangle inequality: $\forall x, y \in E$, $\|x+y\| \leq \|x\| + \|y\|$.

A vector space with a norm is called a normed space. A normed space is a metric space using the metric $d(x, y) = \|x - y\|$.

Example (p-norm on $\mathbb{R}^n$)

The p-norm is defined for $p \geq 1$ for a vector $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ as

$$\|x\|_p = \left(\sum_{i=1}^{n} |x_i|^p \right)^{1/p}$$

when $p=2$, 2-norm = euclidean norm.

The infinity norm is the limit of the p-norm as $p \to \infty$, defined as

$$\|x\|_\infty = \max_i |x_i|$$

Example (p-norm on $C([0,1];\mathbb{R})$)

If we look at the space of continuous functions $C([0,1];\mathbb{R})$, the p-norm is

$$\|f\|_p = \left(\int_0^1 |f(x)|^p \, dx \right)^{1/p}.$$

and the ∞−norm (or sup norm) is

$$\|f\|_\infty = \max_{x \in [0,1]} |f(x)|.$$

Definition

A subset A of a metric space (X, d) is *bounded* if there exists $M > 0$ such that $d(x, y) < M$ for all $x, y \in A$.

Definition

Let (X, d) be a metric space. We define the *open ball* centred at a point $x_0 \in X$ of radius $r > 0$ as

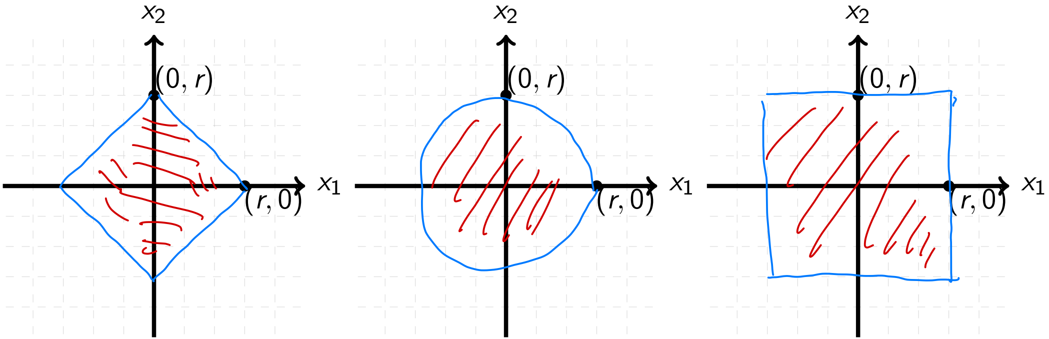
$$B_r(x_0) := \{x \in X : d(x, x_0) < r\}.$$

Example

In $\mathbb{R}$ with the usual norm (absolute value), open balls are symmetric open intervals, i.e.

$$B_r(x_0) = (x_0 - r, x + r)$$

Example: Open ball in $\mathbb{R}^2$ with different metrics



(a) 1-norm (taxicab metric) (b) 2-norm (Euclidean metric) (c) ∞-norm

$d(x,y) = \sum_{i=1}^{2} |x_i - y_i|$

Figure: $B_r(0)$ for different metrics

$\max_i |x_i - y_i|$

References

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