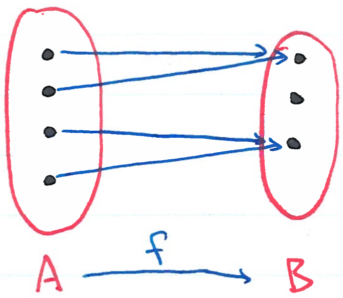
Last time: A function f from a set A to another set B is



a thing which takes inputs from A and produces outputs in B. It can be represented as a subset

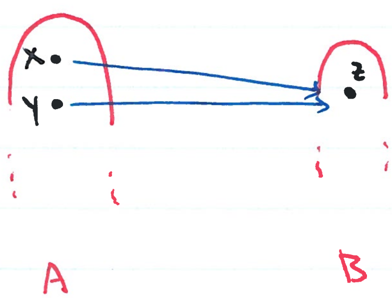
$$f \subseteq A \times B$$

such that
- $\forall a \in A, \exists b \in B$ s.t. $(a,b) \in f$
- $\forall a \in A, \forall b_1, b_2 \in B, \Big(\big((a,b_1) \in f \text{ and } (a,b_2) \in f \big) \Rightarrow b_1 = b_2 \Big)$

Question 1: Given a function $f: A \to B$, can it be "undone"? (I.e. inverted)

Question 2: Can we use a function in order to establish a relationship between the two sets A & B?

Q1: For example, the function drawn above cannot be undone.



To undo it, the element z would both have to go to x AND to y! That's impossible.

Definition: A function $f: A \to B$ is *injective* if ("one-to-one")

$$\forall x, y \in A, \ (x \neq y \Rightarrow f(x) \neq f(y)).$$

Equivalently,

$$\forall x, y \in A, \ (f(x) = f(y) \Rightarrow x = y)$$

(Why is this equivalent?)

Example: $f: \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ is not injective, because $\exists x, y \in \mathbb{R}, (x \neq y \text{ AND } x^2 = y^2)$. For example, $x = 5$ and $y = -5$.

<u>Fun example</u>: Suppose you have a message written in the English alphabet (26 possible letters). You want to <u>encrypt</u> it using numbers, with a one-digit number for each letter (10 possible numbers)

$$\{a, b, c, d, e, \ldots, z\} \xrightarrow{f} \{0, 1, 2, \ldots, 9\}$$

$$A \qquad\qquad\qquad\qquad B$$

Why is this a problem?

<u>A</u>: In order for the message to be decrypted, we would have to "undo" the function (encryption). To do this, f must be injective. But there is no injective function $f: A \to B$ because <u>A has more elements than B</u>! (Any such encryption is "lossy".)

<u>Q2</u>: <u>Fact</u>: If there is an injective function $f: A \to B$, then $|A| \leq |B|$. (For <u>finite</u> sets..)

$\uparrow$ size of A $\qquad$ $\uparrow$ size of B

(Example)

<u>Prop</u>: The function $f: \mathbb{Z} \to \mathbb{Z}$, $f(n) = 3n+1$ is injective.

<u>Pf</u>: Suppose $x, y \in \mathbb{Z}$ are such that $f(x) = f(y)$. Then

$$3x+1 = 3y+1$$

$$\Rightarrow \quad 3x - 3y = 0$$

$$\Rightarrow \quad 3(x-y) = 0$$

$$\Rightarrow \quad x - y = 0 \quad \Rightarrow \quad x = y. \blacksquare$$

<u>Exercise</u>: If $f: A \to B$ is an injective function, then for every $b \in B$, the preimage $f^{-1}(\{b\})$ has size 0 or 1.

"onto"

Definition: A function $f: A \to B$ is surjective if $\forall b \in B, \exists a \in A$ s.t. $f(a) = b$.

- Equivalently, codomain (f) = range (f)
- Equivalently, $\forall b \in B$, the preimage $f^{-1}(\{b\})$ is nonempty.
- "The function f hits every element of B."

Fact: If A, B are finite sets and $f: A \to B$ is a surjective function, then $|A| \geq |B|$.

Example: The function $f: \mathbb{Z} \to \mathbb{Z}$, $f(n) = 3n+1$ is not surjective. For example, $\nexists n \in \mathbb{Z}$, $f(n) = 0$.

Prop: The function $f: \mathbb{R} \to \mathbb{R}$, $f(x) = 3x+1$ is surjective.

Pf: Suppose y is any real number. We must show there is some real number x s.t. $f(x) = y$.
Take $x = \frac{y-1}{3}$. Then $f(x) = 3x+1$

$$= 3\left(\frac{y-1}{3}\right)+1$$

$$= y-1+1 = y. \quad \blacksquare$$

note, the proof essentially proceeded by creating an inverse function!

Definition: A function $f: A \to B$ is called bijective if it is both injective and surjective.

Fact: If A, B are finite sets and $f: A \to B$ is a bijective function, then $|A| = |B|$.

A bijective function is a "perfect matching".

Exercise: For each function, is it injective? Surjective? Bijective?

- $f: [0,\infty) \longrightarrow \mathbb{R}$, $\quad f(x) = x^2$
- $f: \mathbb{R} \longrightarrow [0,\infty)$, $\quad f(x) = x^2$
- $f: [0,\infty) \longrightarrow [0,\infty)$, $\quad f(x) = x^2$

Exercise: Prove that the function $f: \mathbb{R} - \{0\} \longrightarrow \mathbb{R} - \{0\}$, $f(x) = \frac{1}{x}$

is bijective.

Exercise: Prove that the function $f: \mathbb{R} - \{2\} \longrightarrow \mathbb{R} - \{5\}$, $f(x) = \frac{5x+1}{x-2}$

is bijective.