Functions, Pt. 1
Outline for Today

- **What is a Function?**
  - It’s more nuanced than you might expect.

- **Domains and Codomains**
  - Where functions start, and where functions end.

- **Defining a Function**
  - Expressing transformations compactly.

- **Special Classes of Functions**
  - Useful types of functions you’ll encounter IRL.

- **Proofs on First-Order Definitions**
  - A key skill.
What is a function?
Functions, High-School Edition
\[ f(x) = x^4 - 5x^2 + 4 \]
$f(x) = \frac{x^2 + 4x - 9}{x^2 + 10x + 21}$
Functions, High-School Edition

• In high school, functions are usually given as objects of the form

\[ f(x) = \frac{x^3 + 3x^2 + 15x + 7}{1 - x^{137}} \]

• What does a function do?
  • It takes in as input a real number.
  • It outputs a real number
  • ... except when there are vertical asymptotes or other discontinuities, in which case the function doesn't output anything.
Functions, CS Edition
```c
int flipUntil(int n) {
    int numHeads = 0;
    int numTries = 0;

    while (numHeads < n) {
        if (randomBoolean()) {
            numHeads++;
        }
        numTries++;
    }

    return numTries;
}
```
Functions, CS Edition

- In programming, functions
  - might take in inputs,
  - might return values,
  - might have side effects,
  - might never return anything,
  - might crash, and
  - might return different values when called multiple times.
What's Common?

• Although high-school math functions and CS functions are pretty different, they have two key aspects in common:
  • They take in inputs.
  • They produce outputs.
• In logic, we like to keep things simple, so that's pretty much how we're going to define a function.
**High-Level Intuition:**

A function is an object $f$ that takes in exactly one input $x$ and produces exactly one output $f(x)$.

(This is not definition. It’s just to help you build and intuition.)
... but also ...
\[ f(x) = x^2 + 3x - 15 \]
In mathematics, functions are *deterministic*. That is, given the same input, a function must always produce the same output.

The following is a perfectly valid piece of C++ code, but it’s not a valid function under our definition:

```cpp
int randomNumber(int numOutcomes) {
    return rand() % numOutcomes;
}
```
Domains and Codomains

- Every function $f$ has two sets associated with it: its **domain** and its **codomain**.
- A function $f$ can only be applied to elements of its domain. For any $x$ in the domain, $f(x)$ belongs to the codomain.

The function must be defined for every element of the domain.

The output of the function must always be in the codomain, but not all elements of the codomain must be produced as outputs.
Domains and Codomains

- Every function \( f \) has two sets associated with it: its **domain** and its **codomain**.
- A function \( f \) can only be applied to elements of its domain. For any \( x \) in the domain, \( f(x) \) belongs to the codomain.

```java
double absoluteValueOf(double x) {
    if (x >= 0) {
        return x;
    } else {
        return -x;
    }
}
```

The **domain** of this function is \( \mathbb{R} \). Any real number can be provided as input.

The **codomain** of this function is \( \mathbb{R} \). Everything produced is a real number, but not all real numbers can be produced.
Domains and Codomains

- If $f$ is a function whose domain is $A$ and whose codomain is $B$, we write $f : A \rightarrow B$.
- Think of this like a “function prototype” in C++.
Domains and Codomains

- If \( f \) is a function whose domain is \( A \) and whose codomain is \( B \), we write \( f : A \to B \).
- Think of this like a “function prototype” in C++.
The Official Rules for Functions

• Formally speaking, we say that $f : A \rightarrow B$ if the following two rules hold.

• First, $f$ must be obey its domain/codomain rules:
  \[
  \forall a \in A. \exists b \in B. f(a) = b
  \]
  (“Every input in $A$ maps to some output in $B$.”)

• Second, $f$ must be deterministic:
  \[
  \forall a_1 \in A. \forall a_2 \in A. (a_1 = a_2 \rightarrow f(a_1) = f(a_2))
  \]
  (“Equal inputs produce equal outputs.”)

• If you’re ever curious about whether something is a function, look back at these rules and check! For example:
  • Can a function have an empty domain?
  • Can a function have an empty codomain?
Defining Functions
Defining Functions

• To define a function, you need to
  • specify the domain,
  • specify the codomain, and
  • give a rule used to evaluate the function.
• All three pieces are necessary.
  • We need to domain to know what the function can be applied to.
  • We need to codomain to know what the output space is.
  • We need the rule to be able to evaluate the function.
• There are many ways to do this. Let’s go over a few examples.
Functions can be defined as a picture. Draw the domain and codomain explicitly. Then, add arrows to show the outputs.
Functions can be defined as a *rule*. Be sure to explicitly state what the domain and codomain are!

\[ f : \mathbb{Z} \rightarrow \mathbb{Z}, \text{ where} \]
\[ f(x) = x^2 + 3x - 15 \]
Some rules are given piecewise. We select which rule to apply based on the conditions on the right. (Just make sure at least one condition applies and that all applicable conditions give the same result!)

\[ f(n) = \begin{cases} n & \text{if } n \geq 0 \\ -n & \text{if } n \leq 0 \end{cases} \]

\[ f : \mathbb{Z} \to \mathbb{N}, \text{ where} \]
Some Nuances
Is this a function from $\mathbb{R}$ to $\mathbb{R}$?

$$f(x) = \frac{x+2}{x+1}$$
Is this a function from \( \mathbb{R} \) to \( \mathbb{R} \)?

\[
f(x) = \frac{x + 2}{x + 1}
\]

This expression isn’t defined when \( x = -1 \), so \( f \) isn’t defined over its full domain. We therefore don’t consider it to be a function.
Is this a function from $\mathbb{N}$ to $\mathbb{R}$?

$$f(x) = \frac{x+2}{x+1}$$
Is this a function from $\mathbb{N}$ to $\mathbb{R}$?

Yep, it’s a function! Every natural number maps to some real number.

\[
f(x) = \frac{x+2}{x+1}
\]
Is this a function from $A$ to $B$?
Is this a function from $A$ to $B$?
int squigglebah(int input) {
    if (randomCoinTossIsHeads()) {
        return input;
    } else {
        return -input;
    }
}
Is this a function from $\mathbb{Z}$ to $\mathbb{Z}$?

```c
int squigglebah(int input) {
    if (randomCoinTossIsHeads()) {
        return input;
    } else {
        return -input;
    }
}
```

This piece of code is not deterministic. Calling `squigglebah(137)` multiple times might give back different values. It’s therefore not a function in the mathematical sense.
Is this a function from $\mathbb{Z}$ to $\mathbb{Z}$?

```c
int pizkwat(int input) {
    int steps = 0;
    while (input != 0) {
        input -= 2;
        steps++;
    }
    return steps;
}
```
int pizkwat(int input) {
    int steps = 0;
    while (input != 0) {
        input -= 2;
        steps++;
    }
    return steps;
}

This code never produces a value when called on odd input. It’s therefore not defined for all elements of the domain, so it’s not a function in the mathematical sense.

Is this a function from $\mathbb{Z}$ to $\mathbb{Z}$?
Special Types of Functions
What terms are used in this proof? What do they formally mean?

What does this theorem mean? Why, intuitively, should it be true?

What is the standard format for writing a proof? What are the techniques for doing so?
Undoing by Doing Again

- Some operations invert themselves. For example:
  - Flipping a switch twice is the same as not flipping it at all.
  - In first-order logic, \( \neg \neg A \) is equivalent to \( A \).
  - In algebra, \( -(-x) = x \).
  - In set theory, \( (A \Delta B) \Delta B = A \). (*Yes, really!*)

- Operations with these properties are surprisingly useful in CS theory and come up in a bunch of contexts.
  - Storing compressed approximations of sets (XOR filters).
  - Theoretically unbreakable encryption (one-time pads).
  - Transmitting a large file to multiple receivers (fountain codes).
Involutions

• A function \( f : A \rightarrow A \) from a set back to itself is called an **involution** if the following first-order logic statement is true about \( f \):

\[
\forall x \in A. \ f(f(x)) = x.
\]

(“Applying \( f \) twice is equivalent to not applying \( f \) at all.”)

• Involutions have lots of interesting properties. Let’s explore them and see what we can find.
Involutions

Which of the following are involutions?

- $f : \mathbb{Z} \to \mathbb{Z}$ defined as $f(x) = x$.
- $f : \mathbb{Z} \to \mathbb{Z}$ defined as $f(x) = -x$.
- $f : \mathbb{R} \to \mathbb{R}$ defined as $f(x) = \frac{1}{x}$.
- $f : \mathbb{N} \to \mathbb{N}$ defined as follows:
  
  $$f(n) = \begin{cases} 
  n+1 & \text{if } n \text{ is even} \\
  n-1 & \text{if } n \text{ is odd}
  \end{cases}$$

A function $f : A \to A$ is called an involution if the following first-order logic statement is true about $f$:

$$\forall x \in A. \ f(f(x)) = x.$$
Involutions

- Which of the following are involutions?
  - $f : \mathbb{Z} \rightarrow \mathbb{Z}$ defined as $f(x) = x$.
  - $f : \mathbb{Z} \rightarrow \mathbb{Z}$ defined as $f(x) = -x$.
  - $f : \mathbb{R} \rightarrow \mathbb{R}$ defined as $f(x) = \frac{1}{x}$.
  - $f : \mathbb{N} \rightarrow \mathbb{N}$ defined as follows:
    
    $$f(n) = \begin{cases} 
    n+1 & \text{if } n \text{ is even} \\
    n-1 & \text{if } n \text{ is odd}
    \end{cases}$$

A function $f : A \rightarrow A$ is called an involution if the following first-order logic statement is true about $f$:

$$\forall x \in A. \ f(f(x)) = x.$$
Involutions

• Which of the following are involutions?
  • \( f : \mathbb{Z} \to \mathbb{Z} \) defined as \( f(x) = x \). \textit{Yep!}
  • \( f : \mathbb{Z} \to \mathbb{Z} \) defined as \( f(x) = -x \).
  • \( f : \mathbb{R} \to \mathbb{R} \) defined as \( f(x) = \frac{1}{x} \).
  • \( f : \mathbb{N} \to \mathbb{N} \) defined as follows:

\[
  f(n) = \begin{cases} 
  n+1 & \text{if } n \text{ is even} \\
  n-1 & \text{if } n \text{ is odd}
  \end{cases}
\]

A function \( f : A \to A \) is called an \textit{involution} if the following first-order logic statement is true about \( f \):

\[
  \forall x \in A. \; f(f(x)) = x.
\]
A function $f : A \to A$ is called an \textit{involution} if the following first-order logic statement is true about $f$:

$$\forall x \in A. \ f(f(x)) = x.$$
Involutions

Which of the following are involutions?

- $f: \mathbb{Z} \to \mathbb{Z}$ defined as $f(x) = x$. **Yep!**
- $f: \mathbb{Z} \to \mathbb{Z}$ defined as $f(x) = -x$. **Yep!**
- $f: \mathbb{R} \to \mathbb{R}$ defined as $f(x) = \frac{1}{x}$.
- $f: \mathbb{N} \to \mathbb{N}$ defined as follows:

$$f(n) = \begin{cases} n+1 & \text{if } n \text{ is even} \\ n-1 & \text{if } n \text{ is odd} \end{cases}$$

A function $f: A \to A$ is called an **involution** if the following first-order logic statement is true about $f$:

$$\forall x \in A. \ f(f(x)) = x.$$
Involutions

• Which of the following are involutions?
  • \( f : \mathbb{Z} \to \mathbb{Z} \) defined as \( f(x) = x. \) \textit{Yep!}
  • \( f : \mathbb{Z} \to \mathbb{Z} \) defined as \( f(x) = -x. \) \textit{Yep!}
  • \( f : \mathbb{R} \to \mathbb{R} \) defined as \( f(x) = \frac{1}{x}. \)
  • \( f : \mathbb{N} \to \mathbb{N} \) defined as follows:
    \[
    f(n) = \begin{cases} 
      n + 1 & \text{if } n \text{ is even} \\
      n - 1 & \text{if } n \text{ is odd}
    \end{cases}
    \]

A function \( f : A \to A \) is called an \textit{involution} if the following first-order logic statement is true about \( f: \)

\[
\forall x \in A. \ f(f(x)) = x.
\]
Involutions

• Which of the following are involutions?
  • \( f : \mathbb{Z} \rightarrow \mathbb{Z} \) defined as \( f(x) = x \). *Yep!*
  • \( f : \mathbb{Z} \rightarrow \mathbb{Z} \) defined as \( f(x) = -x \). *Yep!*
  • \( f : \mathbb{R} \rightarrow \mathbb{R} \) defined as \( f(x) = \frac{1}{x} \). *Not a function!*
  • \( f : \mathbb{N} \rightarrow \mathbb{N} \) defined as follows:
    \[
    f(n) = \begin{cases} 
    n+1 & \text{if } n \text{ is even} \\
    n-1 & \text{if } n \text{ is odd}
    \end{cases}
    \]

A function \( f : A \rightarrow A \) is called an \textit{involution} if the following first-order logic statement is true about \( f \):

\[
\forall x \in A. \ f(f(x)) = x.
\]
Involutions

• Which of the following are involutions?
  • $f : \mathbb{Z} \rightarrow \mathbb{Z}$ defined as $f(x) = x$. **Yep!**
  • $f : \mathbb{Z} \rightarrow \mathbb{Z}$ defined as $f(x) = -x$. **Yep!**
  • $f : \mathbb{R} \rightarrow \mathbb{R}$ defined as $f(x) = 1/x$. **Not a function!**
  • $f : \mathbb{N} \rightarrow \mathbb{N}$ defined as follows:

$$f(n) = \begin{cases} 
  n+1 & \text{if } n \text{ is even} \\
  n-1 & \text{if } n \text{ is odd}
\end{cases}$$

A function $f : A \rightarrow A$ is called an **involution** if the following first-order logic statement is true about $f$:

$$\forall x \in A. f(f(x)) = x.$$
Involutions

• Which of the following are involutions?
  - \( f : \mathbb{Z} \to \mathbb{Z} \) defined as \( f(x) = x \). \text{Yep!}
  - \( f : \mathbb{Z} \to \mathbb{Z} \) defined as \( f(x) = -x \). \text{Yep!}
  - \( f : \mathbb{R} \to \mathbb{R} \) defined as \( f(x) = \frac{1}{x} \). \text{Not a function!}
  - \( f : \mathbb{N} \to \mathbb{N} \) defined as follows: \text{Yep!}
    \[
    f(n) = \begin{cases} 
    n+1 & \text{if } n \text{ is even} \\
    n-1 & \text{if } n \text{ is odd}
    \end{cases}
    \]

A function \( f : A \to A \) is called an \textit{involution} if the following first-order logic statement is true about \( f \):

\[
\forall x \in A. \ f(f(x)) = x.
\]
Involution

Which of the following are involutions?

- \( f: \mathbb{Z} \to \mathbb{Z} \) defined as \( f(x) = x \). \text{Yep!}
- \( f: \mathbb{Z} \to \mathbb{Z} \) defined as \( f(x) = -x \). \text{Yep!}
- \( f: \mathbb{R} \to \mathbb{R} \) defined as \( f(x) = \frac{1}{x} \). \text{Not a function!}
- \( f: \mathbb{N} \to \mathbb{N} \) defined as follows: \text{Yep!}

\[
f(n) = \begin{cases} 
  n+1 & \text{if } n \text{ is even} \\
  n-1 & \text{if } n \text{ is odd}
\end{cases}
\]

A function \( f: A \to A \) is called an \textit{involution} if the following first-order logic statement is true about \( f \):

\[
\forall x \in A. \ f(f(x)) = x.
\]
Involutions, Visually

A function $f : A \to A$ is called an **involution** if the following first-order logic statement is true about $f$:

$$\forall x \in A. \ f(f(x)) = x.$$
A function $f: A \rightarrow A$ is called an **involution** if the following first-order logic statement is true about $f$:

$$\forall x \in A. f(f(x)) = x.$$
Proofs on Involution
Theorem: The function $f : \mathbb{Z} \rightarrow \mathbb{Z}$ defined as

$$f(n) = \begin{cases} 
  n + 1 & \text{if } n \text{ is even} \\
  n - 1 & \text{if } n \text{ is odd}
\end{cases}$$

is an involution.
**Theorem:** The function $f : \mathbb{Z} \rightarrow \mathbb{Z}$ defined as

\[
f(n) = \begin{cases} 
  n + 1 & \text{if } n \text{ is even} \\
  n - 1 & \text{if } n \text{ is odd}
\end{cases}
\]

is an involution.

**Proof:**

- **Case 1:** $n$ is even. Then $f(n) = n + 1$, which is odd. This means that $f(f(n)) = f(n + 1) = (n + 1) - 1 = n$.
- **Case 2:** $n$ is odd. Then $f(n) = n - 1$, which is even. Then we see that $f(f(n)) = f(n - 1) = (n - 1) + 1 = n$.

In either case, we see that $f(f(n)) = n$, which is what we need to show. ■
Theorem: The function $f : \mathbb{Z} \to \mathbb{Z}$ defined as

$$f(n) = \begin{cases} n+1 & \text{if } n \text{ is even} \\ n-1 & \text{if } n \text{ is odd} \end{cases}$$

is an involution.

Proof:

What does it mean for $f$ to be an involution?
**Theorem:** The function \( f : \mathbb{Z} \to \mathbb{Z} \) defined as

\[
    f(n) = \begin{cases} 
        n + 1 & \text{if } n \text{ is even} \\
        n - 1 & \text{if } n \text{ is odd}
    \end{cases}
\]

is an involution.

**Proof:**

What does it mean for \( f \) to be an involution?

\[
    \forall n \in \mathbb{Z}. \ f(f(n)) = n.
\]
**Theorem:** The function $f : \mathbb{Z} \to \mathbb{Z}$ defined as

$$f(n) = \begin{cases}  
  n+1 & \text{if } n \text{ is even} \\
  n-1 & \text{if } n \text{ is odd}
\end{cases}$$

is an involution.

**Proof:**

What does it mean for $f$ to be an involution?

$$\forall n \in \mathbb{Z}. \ f(f(n)) = n.$$ 

Therefore, we’ll have the reader pick some $n \in \mathbb{Z}$, then argue that $f(f(n)) = n$. 
Theorem: The function \( f : \mathbb{Z} \rightarrow \mathbb{Z} \) defined as

\[
  f(n) = \begin{cases} 
    n+1 & \text{if } n \text{ is even} \\
    n-1 & \text{if } n \text{ is odd}
  \end{cases}
\]

is an involution.

Proof:

What does it mean for \( f \) to be an involution?

\[
  \forall n \in \mathbb{Z}. \ f(f(n)) = n.
\]

Therefore, we’ll have the reader pick some \( n \in \mathbb{Z} \), then argue that \( f(f(n)) = n \).
**Theorem:** The function $f: \mathbb{Z} \to \mathbb{Z}$ defined as

$$f(n) = \begin{cases} n+1 & \text{if } n \text{ is even} \\ n-1 & \text{if } n \text{ is odd} \end{cases}$$

is an involution.

**Proof:**

What does it mean for $f$ to be an involution?

$$\forall n \in \mathbb{Z}. \quad f(f(n)) = n.$$

Therefore, we’ll have the reader pick some $n \in \mathbb{Z}$, then argue that $f(f(n)) = n$. 
**Theorem:** The function $f : \mathbb{Z} \to \mathbb{Z}$ defined as

$$f(n) = \begin{cases} 
  n+1 & \text{if } n \text{ is even} \\
  n-1 & \text{if } n \text{ is odd}
\end{cases}$$

is an involution.

**Proof:**

What does it mean for $f$ to be an involution?

$$\forall n \in \mathbb{Z}. \ f(f(n)) = n.$$  

Therefore, we’ll have the reader pick some $n \in \mathbb{Z}$, then argue that $f(f(n)) = n$. 

**Theorem:** The function $f : \mathbb{Z} \rightarrow \mathbb{Z}$ defined as

$$f(n) = \begin{cases} 
  n+1 & \text{if } n \text{ is even} \\
  n-1 & \text{if } n \text{ is odd}
\end{cases}$$

is an involution.

**Proof:** Pick some $n \in \mathbb{Z}$. 

\[ f(f(n)) = \begin{cases} 
  n+1 & \text{if } n \text{ is even} \\
  n-1 & \text{if } n \text{ is odd}
\end{cases} = n \]

In either case, we see that $f(f(n)) = n$, which is what we need to show. ■
**Theorem:** The function $f : \mathbb{Z} \to \mathbb{Z}$ defined as

$$f(n) = \begin{cases} n+1 & \text{if } n \text{ is even} \\ n-1 & \text{if } n \text{ is odd} \end{cases}$$

is an involution.

**Proof:** Pick some $n \in \mathbb{Z}$. We need to show that $f(f(n)) = n$. 
Theorem: The function $f: \mathbb{Z} \to \mathbb{Z}$ defined as

$$f(n) = \begin{cases} 
  n+1 & \text{if } n \text{ is even} \\
  n-1 & \text{if } n \text{ is odd}
\end{cases}$$

is an involution.

Proof: Pick some $n \in \mathbb{Z}$. We need to show that $f(f(n)) = n$. To do so, we consider two cases.

Case 1: $n$ is even.

Case 2: $n$ is odd.
**Theorem:** The function $f : \mathbb{Z} \rightarrow \mathbb{Z}$ defined as

$$f(n) = \begin{cases} 
  n+1 & \text{if } n \text{ is even} \\
  n-1 & \text{if } n \text{ is odd} 
\end{cases}$$

is an involution.

**Proof:** Pick some $n \in \mathbb{Z}$. We need to show that $f(f(n)) = n$. To do so, we consider two cases.

Case 1: $n$ is even. Then $f(n) = n+1$, which is odd.

Case 2: $n$ is odd.
**Theorem:** The function $f : \mathbb{Z} \to \mathbb{Z}$ defined as

$$f(n) = \begin{cases} 
  n+1 & \text{if } n \text{ is even} \\
  n-1 & \text{if } n \text{ is odd}
\end{cases}$$

is an involution.

**Proof:** Pick some $n \in \mathbb{Z}$. We need to show that $f(f(n)) = n$. To do so, we consider two cases.

*Case 1:* $n$ is even. Then $f(n) = n+1$, which is odd. This means that $f(f(n)) = f(n+1) = (n+1) - 1 = n$.

*Case 2:* $n$ is odd.
**Theorem:** The function $f : \mathbb{Z} \to \mathbb{Z}$ defined as

$$f(n) = \begin{cases} n+1 & \text{if } n \text{ is even} \\ n-1 & \text{if } n \text{ is odd} \end{cases}$$

is an involution.

**Proof:** Pick some $n \in \mathbb{Z}$. We need to show that $f(f(n)) = n$. To do so, we consider two cases.

*Case 1:* $n$ is even. Then $f(n) = n+1$, which is odd. This means that $f(f(n)) = f(n+1) = (n+1) - 1 = n$.

*Case 2:* $n$ is odd. Then $f(n) = n - 1$, which is even.
**Theorem:** The function $f : \mathbb{Z} \to \mathbb{Z}$ defined as

$$f(n) = \begin{cases} n+1 & \text{if } n \text{ is even} \\ n-1 & \text{if } n \text{ is odd} \end{cases}$$

is an involution.

**Proof:** Pick some $n \in \mathbb{Z}$. We need to show that $f(f(n)) = n$. To do so, we consider two cases.

*Case 1:* $n$ is even. Then $f(n) = n+1$, which is odd. This means that $f(f(n)) = f(n+1) = (n+1) - 1 = n$.

*Case 2:* $n$ is odd. Then $f(n) = n - 1$, which is even. Then we see that $f(f(n)) = f(n - 1) = (n - 1) + 1 = n$. 


**Theorem:** The function \( f : \mathbb{Z} \to \mathbb{Z} \) defined as

\[
f(n) = \begin{cases} 
  n+1 & \text{if } n \text{ is even} \\
  n-1 & \text{if } n \text{ is odd}
\end{cases}
\]

is an involution.

**Proof:** Pick some \( n \in \mathbb{Z} \). We need to show that \( f(f(n)) = n \). To do so, we consider two cases.

*Case 1:* \( n \) is even. Then \( f(n) = n+1 \), which is odd. This means that \( f(f(n)) = f(n+1) = (n+1) - 1 = n \).

*Case 2:* \( n \) is odd. Then \( f(n) = n - 1 \), which is even. Then we see that \( f(f(n)) = f(n - 1) = (n - 1) + 1 = n \).

In either case, we see that \( f(f(n)) = n \), which is what we need to show.
Theorem: The function $f : \mathbb{Z} \to \mathbb{Z}$ defined as

$$f(n) = \begin{cases} n+1 & \text{if } n \text{ is even} \\ n-1 & \text{if } n \text{ is odd} \end{cases}$$

is an involution.

Proof: Pick some $n \in \mathbb{Z}$. We need to show that $f(f(n)) = n$. To do so, we consider two cases.

Case 1: $n$ is even. Then $f(n) = n+1$, which is odd. This means that $f(f(n)) = f(n+1) = (n+1) - 1 = n$.

Case 2: $n$ is odd. Then $f(n) = n - 1$, which is even. Then we see that $f(f(n)) = f(n - 1) = (n - 1) + 1 = n$.

In either case, we see that $f(f(n)) = n$, which is what we need to show. ■
Theorem: The function \( f : \mathbb{Z} \to \mathbb{Z} \) defined as

\[
  f(n) = \begin{cases} 
    n + 1 & \text{if } n \text{ is even} \\
    n - 1 & \text{if } n \text{ is odd}
  \end{cases}
\]

is an involution.

Proof: Pick some \( n \in \mathbb{Z} \). We need to show that \( f(f(n)) = n \). To do so, we consider two cases.

Case 1: \( n \) is even. Then \( f(n) = n + 1 \), which is odd. This means that \( f(f(n)) = f(n + 1) = (n + 1) - 1 = n \).

Case 2: \( n \) is odd. Then \( f(n) = n - 1 \), which is even. Then we see that \( f(f(n)) = f(n - 1) = (n - 1) + 1 = n \).

In either case, we see that \( f(f(n)) = n \), which is what we need to show. \( \blacksquare \)
To *prove* that this is true...
To *prove* that this is true...

<table>
<thead>
<tr>
<th>$\forall x. A$</th>
<th>Have the reader pick an arbitrary $x$. We then prove $A$ is true for that choice of $x$.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Theorem:** The function $f : \mathbb{N} \rightarrow \mathbb{N}$ defined as $f(n) = n^2$ is not an involution.
Theorem: The function \( f : \mathbb{N} \rightarrow \mathbb{N} \) defined as \( f(n) = n^2 \) is not an involution.

What does it mean for \( f \) to be an involution?

\[
\forall n \in \mathbb{N}. \; f(f(n)) = n.
\]

What is the negation of this statement?

\[
\neg \forall n \in \mathbb{N}. \; f(f(n)) = n \\
\exists n \in \mathbb{N}. \; \neg (f(f(n)) = n) \\
\exists n \in \mathbb{N}. \; f(f(n)) \neq n
\]

Therefore, we need to pick some concrete choice of \( n \) such that \( f(f(n)) \neq n \).
**Theorem:** The function \( f : \mathbb{N} \to \mathbb{N} \) defined as \( f(n) = n^2 \) is not an involution.

What does it mean for \( f \) to be an involution?

\[ \forall n \in \mathbb{N}. \ f(f(n)) = n. \]

What is the negation of this statement?

\[ \neg \forall n \in \mathbb{N}. \ f(f(n)) = n \]
\[ \exists n \in \mathbb{N}. \ \neg (f(f(n)) = n) \]
\[ \exists n \in \mathbb{N}. \ f(f(n)) \neq n \]

Therefore, we need to pick some concrete choice of \( n \) such that \( f(f(n)) \neq n \).
**Theorem:** The function \( f : \mathbb{N} \to \mathbb{N} \) defined as \( f(n) = n^2 \) is not an involution.

What does it mean for \( f \) to be an involution?

\[
\forall n \in \mathbb{N}. \ f(f(n)) = n.
\]

What is the negation of this statement?

\[
\neg \forall n \in \mathbb{N}. \ f(f(n)) = n \\
\exists n \in \mathbb{N}. \ \neg (f(f(n)) = n) \\
\exists n \in \mathbb{N}. \ f(f(n)) \neq n
\]

Therefore, we need to pick some concrete choice of \( n \) such that \( f(f(n)) \neq n \).
**Theorem:** The function $f : \mathbb{N} \to \mathbb{N}$ defined as $f(n) = n^2$ is not an involution.

What does it mean for $f$ to be an involution?

$$\forall n \in \mathbb{N}. f(f(n)) = n.$$

What is the negation of this statement?

$$\neg \forall n \in \mathbb{N}. f(f(n)) = n$$

$$\exists n \in \mathbb{N}. \neg(f(f(n)) = n)$$

$$\exists n \in \mathbb{N}. f(f(n)) \neq n$$

Therefore, we need to pick some concrete choice of $n$ such that $f(f(n)) \neq n$. 
**Theorem:** The function $f : \mathbb{N} \to \mathbb{N}$ defined as $f(n) = n^2$ is not an involution.

**Proof:** We need to show that there is some $n \in \mathbb{N}$ where $f(f(n)) \neq n$.

Pick $n = 2$. Then

$$f \left( f(n) \right) = f(f(2))$$
$$= f(4)$$
$$= 16,$$

which means that $f(f(n)) \neq 2$, as required. ■
**Theorem:** The function $f : \mathbb{N} \rightarrow \mathbb{N}$ defined as $f(n) = n^2$ is not an involution.

**Proof:** We need to show that there is some $n \in \mathbb{N}$ where $f(f(n)) \neq n$.

Pick $n = 2$. Then

$$f (f(n)) = f(f(2))$$
$$= f(4)$$
$$= 16,$$

which means that $f(f(n)) \neq 2$, as required. ■

This proof contains no first-order logic syntax (quantifiers, connectives, etc.). It’s written in plain English, just as usual.
To *prove* that this is true...

| ∀x. A | Have the reader pick an arbitrary x. We then prove A is true for that choice of x. |
To *prove* that this is true...

| \( \forall x. A \) | Have the reader pick an arbitrary \( x \). We then prove \( A \) is true for that choice of \( x \). |
| \( \neg A \) | Simplify the negation, then consult this table on the result. |
To *prove* that this is true...

| $\forall x. A$ | Have the reader pick an arbitrary $x$. We then prove $A$ is true for that choice of $x$. |
| $\exists x. A$ | Find an $x$ where $A$ is true. Then prove that $A$ is true for that specific choice of $x$. |
| $\neg A$ | Simplify the negation, then consult this table on the result. |
Another Class of Functions
Injective Functions

• A function $f : A \rightarrow B$ is called **injective** (or **one-to-one**) if the following statement is true about $f$:

  $\forall a_1 \in A. \forall a_2 \in A. (a_1 \neq a_2 \rightarrow f(a_1) \neq f(a_2))$

  ("If the inputs are different, the outputs are different.")

• The following first-order definition is equivalent (why?) and is often useful in proofs.

  $\forall a_1 \in A. \forall a_2 \in A. (f(a_1) = f(a_2) \rightarrow a_1 = a_2)$

  ("If the outputs are the same, the inputs are the same.")

• A function with this property is called an **injection**.

• How does this compare to our second rule for functions?
Injections

• Let ♦ be the set of all CS103 students. Which of the following are injective?
  • $f : ♦ \rightarrow \mathbb{N}$ where $f(x)$ is $x$’s Stanford ID number.
  • $f : ♦ \rightarrow \exists$ where $\exists$ is the set of all countries and $f(x)$ is $x$’s country of birth.
  • $f : ♦ \rightarrow \rightarrow$ where $\rightarrow$ is the set of all given (first) names, where $f(x)$ is $x$’s given (first) name.

A function $f : A \rightarrow B$ is **injective** if either statement is true:

$$\forall x_1 \in A. \forall x_2 \in A. (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))$$

$$\forall x_1 \in A. \forall x_2 \in A. (f(x_1) = f(x_2) \rightarrow x_1 = x_2)$$
Injections

- Let be the set of all CS103 students.
  Which of the following are injective?

  ✔ • \( f : \rightarrow \mathbb{N} \) where \( f(x) \) is \( x \)'s Stanford ID number.
  • \( f : \rightarrow \) where \( f(x) \) is \( x \)'s country of birth.
  • \( f : \rightarrow \) where \( f(x) \) is \( x \)'s given (first) name.

A function \( f : A \rightarrow B \) is **injective** if either statement is true:

\[
\forall x_1 \in A. \forall x_2 \in A. (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))
\]
\[
\forall x_1 \in A. \forall x_2 \in A. (f(x_1) = f(x_2) \rightarrow x_1 = x_2)
\]


Injections

• Let be the set of all CS103 students. Which of the following are injective?
   ✔ • \( f : A \rightarrow \mathbb{N} \) where \( f(x) \) is \( x \)'s Stanford ID number.
   ✗ • \( f : A \rightarrow \mathbb{C} \) where \( \mathbb{C} \) is the set of all countries and \( f(x) \) is \( x \)'s country of birth.
   • \( f : A \rightarrow \mathbb{N} \) where \( \mathbb{N} \) is the set of all given (first) names, where \( f(x) \) is \( x \)'s given (first) name.

A function \( f : A \rightarrow B \) is **injective** if either statement is true:

\[
\forall x_1 \in A. \forall x_2 \in A. (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))
\]

\[
\forall x_1 \in A. \forall x_2 \in A. (f(x_1) = f(x_2) \rightarrow x_1 = x_2)
\]
Injections

Let be the set of all CS103 students. Which of the following are injective?

✔ • \( f : \mathbb{N} \to \mathbb{N} \) where \( f(x) \) is \( x \)'s Stanford ID number.

❌ • \( f : \mathbb{N} \to \mathbb{N} \) where \( f(x) \) is \( x \)'s country of birth.

❌ • \( f : \mathbb{N} \to \mathbb{N} \) where \( f(x) \) is \( x \)'s given (first) name.

A function \( f : A \to B \) is injective if either statement is true:

\[
\forall x_1 \in A. \forall x_2 \in A. (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))
\]

\[
\forall x_1 \in A. \forall x_2 \in A. (f(x_1) = f(x_2) \rightarrow x_1 = x_2)
\]
Injections

• Let be the set of all CS103 students. Which of the following are injective?

✔ • \( f: \text{CS103 students} \rightarrow \mathbb{N} \) where \( f(x) \) is \( x \)'s Stanford ID number.

❌ • \( f: \text{CS103 students} \rightarrow \text{Countries} \) where \( f(x) \) is \( x \)'s country of birth.

❌ • \( f: \text{CS103 students} \rightarrow \text{First names} \) where \( f(x) \) is \( x \)'s given (first) name.

A function \( f: A \rightarrow B \) is **injective** if either statement is true:

\[
\forall x_1 \in A. \forall x_2 \in A. (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))
\]

\[
\forall x_1 \in A. \forall x_2 \in A. (f(x_1) = f(x_2) \rightarrow x_1 = x_2)
\]
Injective Functions

**Theorem:** Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then $f$ is injective.
Injective Functions

**Theorem:** Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then $f$ is injective.

**Proof:**

Given any $n_0, n_1 \in \mathbb{N}$ where $f(n_0) = f(n_1)$, we will prove that $n_0 = n_1$.

Since $f(n_0) = f(n_1)$, we see that $2n_0 + 7 = 2n_1 + 7$.

This in turn means that $2n_0 = 2n_1$, so $n_0 = n_1$, as required. $\square$
Injective Functions

**Theorem:** Let $f : \mathbb{N} \rightarrow \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then $f$ is injective.

**Proof:**

What does it mean for the function $f$ to be injective?
Injective Functions

**Theorem:** Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then $f$ is injective.

**Proof:**

What does it mean for the function $f$ to be injective?

$\forall n_1 \in \mathbb{N}. \forall n_2 \in \mathbb{N}. ( f(n_1) = f(n_2) \rightarrow n_1 = n_2 )$

$\forall n_1 \in \mathbb{N}. \forall n_2 \in \mathbb{N}. ( n_1 \neq n_2 \rightarrow f(n_1) \neq f(n_2) )$
Injective Functions

**Theorem:** Let \( f : \mathbb{N} \to \mathbb{N} \) be defined as \( f(n) = 2n + 7 \). Then \( f \) is injective.

**Proof:**

What does it mean for the function \( f \) to be injective?

\[
\forall n_1 \in \mathbb{N}. \forall n_2 \in \mathbb{N}. ( f(n_1) = f(n_2) \rightarrow n_1 = n_2 )
\]

\[
\forall n_1 \in \mathbb{N}. \forall n_2 \in \mathbb{N}. ( n_1 \neq n_2 \rightarrow f(n_1) \neq f(n_2) )
\]
Injective Functions

**Theorem:** Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then $f$ is injective.

**Proof:**

What does it mean for the function $f$ to be injective?

\[
\forall n_1 \in \mathbb{N}. \forall n_2 \in \mathbb{N}. \ ( f(n_1) = f(n_2) \rightarrow n_1 = n_2 )
\]
\[
\forall n_1 \in \mathbb{N}. \forall n_2 \in \mathbb{N}. \ ( n_1 \neq n_2 \rightarrow f(n_1) \neq f(n_2) )
\]

Therefore, we'll pick arbitrary $n_1, n_2 \in \mathbb{N}$, assume $f(n_1) = f(n_2)$, then prove that $n_1 = n_2$. 

Injective Functions

**Theorem:** Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then $f$ is injective.

**Proof:**

What does it mean for the function $f$ to be injective?

\[ \forall n_1 \in \mathbb{N}. \forall n_2 \in \mathbb{N}. ( f(n_1) = f(n_2) \rightarrow n_1 = n_2 ) \]
\[ \forall n_1 \in \mathbb{N}. \forall n_2 \in \mathbb{N}. ( n_1 \neq n_2 \rightarrow f(n_1) \neq f(n_2) ) \]

Therefore, we'll pick arbitrary $n_1, n_2 \in \mathbb{N}$, assume $f(n_1) = f(n_2)$, then prove that $n_1 = n_2$. 
Injective Functions

**Theorem:** Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then $f$ is injective.

**Proof:**

What does it mean for the function $f$ to be injective?

\[
\forall n_1 \in \mathbb{N}. \forall n_2 \in \mathbb{N}. ( f(n_1) = f(n_2) \rightarrow n_1 = n_2 )
\]
\[
\forall n_1 \in \mathbb{N}. \forall n_2 \in \mathbb{N}. ( n_1 \neq n_2 \rightarrow f(n_1) \neq f(n_2) )
\]

Therefore, we'll pick arbitrary $n_1, n_2 \in \mathbb{N}$, assume $f(n_1) = f(n_2)$, then prove that $n_1 = n_2$. 
Injective Functions

**Theorem:** Let \( f : \mathbb{N} \rightarrow \mathbb{N} \) be defined as \( f(n) = 2n + 7 \). Then \( f \) is injective.

**Proof:**

What does it mean for the function \( f \) to be injective?

\[
\forall n_1 \in \mathbb{N}. \forall n_2 \in \mathbb{N}. \ ( f(n_1) = f(n_2) \rightarrow n_1 = n_2 )
\]

\[
\forall n_1 \in \mathbb{N}. \forall n_2 \in \mathbb{N}. \ ( n_1 \neq n_2 \rightarrow f(n_1) \neq f(n_2) )
\]

Therefore, we'll pick arbitrary \( n_1, n_2 \in \mathbb{N} \), assume \( f(n_1) = f(n_2) \), then prove that \( n_1 = n_2 \).
Injective Functions

**Theorem:** Let $f : \mathbb{N} \rightarrow \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then $f$ is injective.

**Proof:** Consider any $n_1, n_2 \in \mathbb{N}$ where $f(n_1) = f(n_2)$. We will prove that $n_1 = n_2$. 
Theorem: Let \( f : \mathbb{N} \rightarrow \mathbb{N} \) be defined as \( f(n) = 2n + 7 \). Then \( f \) is injective.

Proof: Consider any \( n_1, n_2 \in \mathbb{N} \) where \( f(n_1) = f(n_2) \). We will prove that \( n_1 = n_2 \).

Since \( f(n_1) = f(n_2) \), we see that

\[
2n_1 + 7 = 2n_2 + 7.
\]
Injective Functions

**Theorem:** Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then $f$ is injective.

**Proof:** Consider any $n_1, n_2 \in \mathbb{N}$ where $f(n_1) = f(n_2)$. We will prove that $n_1 = n_2$.

Since $f(n_1) = f(n_2)$, we see that

$$2n_1 + 7 = 2n_2 + 7.$$

This in turn means that

$$2n_1 = 2n_2$$
Injective Functions

**Theorem:** Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then $f$ is injective.

**Proof:** Consider any $n_1, n_2 \in \mathbb{N}$ where $f(n_1) = f(n_2)$. We will prove that $n_1 = n_2$.

Since $f(n_1) = f(n_2)$, we see that

$$2n_1 + 7 = 2n_2 + 7.$$  

This in turn means that

$$2n_1 = 2n_2,$$

so $n_1 = n_2$, as required.
Injective Functions

**Theorem:** Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then $f$ is injective.

**Proof:** Consider any $n_1, n_2 \in \mathbb{N}$ where $f(n_1) = f(n_2)$. We will prove that $n_1 = n_2$.

Since $f(n_1) = f(n_2)$, we see that

$$2n_1 + 7 = 2n_2 + 7.$$

This in turn means that

$$2n_1 = 2n_2,$$

so $n_1 = n_2$, as required. ■

Good exercise: Repeat this proof using the other definition of injectivity!
Injective Functions

**Theorem:** Let $f : \mathbb{N} \rightarrow \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then $f$ is injective.

**Proof:** Consider any $n_1, n_2 \in \mathbb{N}$ where $f(n_1) = f(n_2)$. We will prove that $n_1 = n_2$.

Since $f(n_1) = f(n_2)$, we see that

$$2n_1 + 7 = 2n_2 + 7.$$  

This in turn means that

$$2n_1 = 2n_2,$$

so $n_1 = n_2$, as required. ■

This proof contains no first-order logic syntax (quantifiers, connectives, etc.). It’s written in plain English, just as usual.
<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\forall x. A$</td>
<td>Have the reader pick an arbitrary $x$. We then prove $A$ is true for that choice of $x$.</td>
</tr>
<tr>
<td>$\exists x. A$</td>
<td>Find an $x$ where $A$ is true. Then prove that $A$ is true for that specific choice of $x$.</td>
</tr>
<tr>
<td>$\neg A$</td>
<td>Simplify the negation, then consult this table on the result.</td>
</tr>
</tbody>
</table>
To *prove* that this is true...

| \( \forall x. A \) | Have the reader pick an arbitrary \( x \). We then prove \( A \) is true for that choice of \( x \). |
| \( \exists x. A \) | Find an \( x \) where \( A \) is true. Then prove that \( A \) is true for that specific choice of \( x \). |
| \( A \rightarrow B \) | Assume \( A \) is true, then prove \( B \) is true. |
| \( \neg A \) | Simplify the negation, then consult this table on the result. |
Injective Functions

**Theorem:** Let $f : \mathbb{Z} \rightarrow \mathbb{N}$ be defined as $f(x) = x^4$. Then $f$ is not injective.
Injective Functions

**Theorem:** Let \( f : \mathbb{Z} \to \mathbb{N} \) be defined as \( f(x) = x^4 \). Then \( f \) is not injective.

**Proof:**
Injective Functions

**Theorem:** Let $f : \mathbb{Z} \to \mathbb{N}$ be defined as $f(x) = x^4$. Then $f$ is not injective.

**Proof:**

What does it mean for $f$ to be injective?

$\forall x_1 \in \mathbb{Z}. \forall x_2 \in \mathbb{Z}. (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))$

What is the negation of this statement?

$\neg \forall x_1 \in \mathbb{Z}. \forall x_2 \in \mathbb{Z}. (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))$

$\exists x_1 \in \mathbb{Z}. \neg \forall x_2 \in \mathbb{Z}. (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))$

$\exists x_1 \in \mathbb{Z}. \exists x_2 \in \mathbb{Z}. \neg (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))$

$\exists x_1 \in \mathbb{Z}. \exists x_2 \in \mathbb{Z}. (x_1 \neq x_2 \land \neg (f(x_1) \neq f(x_2)))$

$\exists x_1 \in \mathbb{Z}. \exists x_2 \in \mathbb{Z}. (x_1 \neq x_2 \land f(x_1) = f(x_2))$

Therefore, we need to find $x_1, x_2 \in \mathbb{Z}$ such that $x_1 \neq x_2$, but $f(x_1) = f(x_2)$. Can we do that?
Injective Functions

**Theorem:** Let $f : \mathbb{Z} \to \mathbb{N}$ be defined as $f(x) = x^4$. Then $f$ is not injective.

**Proof:**

What does it mean for $f$ to be injective?

$$
\forall x_1 \in \mathbb{Z}. \forall x_2 \in \mathbb{Z}. (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))
$$

What is the negation of this statement?

$$
\neg \forall x_1 \in \mathbb{Z}. \forall x_2 \in \mathbb{Z}. (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))
$$

$$
\exists x_1 \in \mathbb{Z}. \exists x_2 \in \mathbb{Z}. (x_1 \neq x_2 \land \neg (f(x_1) \neq f(x_2)))
$$

Therefore, we need to find $x_1, x_2 \in \mathbb{Z}$ such that $x_1 \neq x_2$, but $f(x_1) = f(x_2)$. Can we do that?
Injective Functions

**Theorem:** Let $f : \mathbb{Z} \to \mathbb{N}$ be defined as $f(x) = x^4$. Then $f$ is not injective.

**Proof:**

What does it mean for $f$ to be injective?

$$\forall x_1 \in \mathbb{Z}. \forall x_2 \in \mathbb{Z}. (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))$$

What is the negation of this statement?

$$\neg \forall x_1 \in \mathbb{Z}. \forall x_2 \in \mathbb{Z}. (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))$$

Therefore, we need to find $x_1, x_2 \in \mathbb{Z}$ such that $x_1 \neq x_2$, but $f(x_1) = f(x_2)$. Can we do that?
Injective Functions

**Theorem:** Let \( f : \mathbb{Z} \to \mathbb{N} \) be defined as \( f(x) = x^4 \). Then \( f \) is not injective.

**Proof:**

What does it mean for \( f \) to be injective?

\[
\forall x_1 \in \mathbb{Z}. \forall x_2 \in \mathbb{Z}. \ (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))
\]

What is the negation of this statement?

\[
\neg \forall x_1 \in \mathbb{Z}. \forall x_2 \in \mathbb{Z}. \ (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))
\]

\[
\exists x_1 \in \mathbb{Z}. \neg \forall x_2 \in \mathbb{Z}. \ (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))
\]

\[
\exists x_1 \in \mathbb{Z}. \exists x_2 \in \mathbb{Z}. \neg (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))
\]

\[
\exists x_1 \in \mathbb{Z}. \exists x_2 \in \mathbb{Z}. \ (x_1 \neq x_2 \land \neg (f(x_1) \neq f(x_2)))
\]

\[
\exists x_1 \in \mathbb{Z}. \exists x_2 \in \mathbb{Z}. \ (x_1 \neq x_2 \land f(x_1) = f(x_2))
\]

Therefore, we need to find \( x_1, x_2 \in \mathbb{Z} \) such that \( x_1 \neq x_2 \), but \( f(x_1) = f(x_2) \). Can we do that?
Injective Functions

Theorem: Let $f : \mathbb{Z} \to \mathbb{N}$ be defined as $f(x) = x^4$. Then $f$ is not injective.

Proof: We will prove that there exist integers $x_1$ and $x_2$ such that $x_1 \neq x_2$, but $f(x_1) = f(x_2)$. Let $x_0 = -1$ and $x_1 = 1$. Then $f(x_0) = f(-1) = (-1)^4 = 1$ and $f(x_1) = f(1) = 1^4 = 1$, so $f(x_0) = f(x_1)$ even though $x_0 \neq x_1$, as required. ■
Injective Functions

**Theorem:** Let $f : \mathbb{Z} \to \mathbb{N}$ be defined as $f(x) = x^4$. Then $f$ is not injective.

**Proof:** We will prove that there exist integers $x_1$ and $x_2$ such that $x_1 \neq x_2$, but $f(x_1) = f(x_2)$.

Let $x_1 = -1$ and $x_2 = +1$. 

---

$\sqrt{1}$
Injective Functions

**Theorem:** Let $f : \mathbb{Z} \to \mathbb{N}$ be defined as $f(x) = x^4$. Then $f$ is not injective.

**Proof:** We will prove that there exist integers $x_1$ and $x_2$ such that $x_1 \neq x_2$, but $f(x_1) = f(x_2)$.

Let $x_1 = -1$ and $x_2 = +1$. Notice that

$$f(x_1) = f(-1) = (-1)^4 = 1$$

and

$$f(x_2) = f(1) = 1^4 = 1,$$

so $f(x_0) = f(x_1)$ even though $x_0 \neq x_1$, as required. ■
Injective Functions

**Theorem:** Let $f : \mathbb{Z} \to \mathbb{N}$ be defined as $f(x) = x^4$. Then $f$ is not injective.

**Proof:** We will prove that there exist integers $x_1$ and $x_2$ such that $x_1 \neq x_2$, but $f(x_1) = f(x_2)$.

Let $x_1 = -1$ and $x_2 = +1$. Notice that

$$f(x_1) = f(-1) = (-1)^4 = 1$$

and

$$f(x_2) = f(1) = 1^4 = 1$$
Injective Functions

**Theorem:** Let $f : \mathbb{Z} \to \mathbb{N}$ be defined as $f(x) = x^4$. Then $f$ is not injective.

**Proof:** We will prove that there exist integers $x_1$ and $x_2$ such that $x_1 \neq x_2$, but $f(x_1) = f(x_2)$.

Let $x_1 = -1$ and $x_2 = +1$. Notice that

$$f(x_1) = f(-1) = (-1)^4 = 1$$

and

$$f(x_2) = f(1) = 1^4 = 1,$$

so $f(x_1) = f(x_2)$ even though $x_1 \neq x_2$, as required.
Theorem: Let $f : \mathbb{Z} \rightarrow \mathbb{N}$ be defined as $f(x) = x^4$. Then $f$ is not injective.

Proof: We will prove that there exist integers $x_1$ and $x_2$ such that $x_1 \neq x_2$, but $f(x_1) = f(x_2)$.

Let $x_1 = -1$ and $x_2 = +1$. Notice that

$$f(x_1) = f(-1) = (-1)^4 = 1$$

and

$$f(x_2) = f(1) = 1^4 = 1,$$

so $f(x_1) = f(x_2)$ even though $x_1 \neq x_2$, as required. ■
Injective Functions

**Theorem:** Let \( f : \mathbb{Z} \to \mathbb{N} \) be defined as \( f(x) = x^4 \). Then \( f \) is not injective.

**Proof:** We will prove that there exist integers \( x_1 \) and \( x_2 \) such that \( x_1 \neq x_2 \), but \( f(x_1) = f(x_2) \).

Let \( x_1 = -1 \) and \( x_2 = +1 \). Notice that

\[
f(x_1) = f(-1) = (-1)^4 = 1
\]

and

\[
f(x_2) = f(1) = 1^4 = 1,
\]

so \( f(x_1) = f(x_2) \) even though \( x_1 \neq x_2 \).
To *prove* that this is true...

<table>
<thead>
<tr>
<th>∀ x. A</th>
<th>Have the reader pick an arbitrary <em>x</em>. We then prove <em>A</em> is true for that choice of <em>x</em>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>∃ x. A</td>
<td>Find an <em>x</em> where <em>A</em> is true. Then prove that <em>A</em> is true for that specific choice of <em>x</em>.</td>
</tr>
<tr>
<td>A → B</td>
<td>Assume <em>A</em> is true, then prove <em>B</em> is true.</td>
</tr>
</tbody>
</table>

Simplify the negation, then consult this table on the result.
| \( \forall x. A \) | Have the reader pick an arbitrary \( x \). We then prove \( A \) is true for that choice of \( x \). |
| \( \exists x. A \) | Find an \( x \) where \( A \) is true. Then prove that \( A \) is true for that specific choice of \( x \). |
| \( A \rightarrow B \) | Assume \( A \) is true, then prove \( B \) is true. |
| \( A \land B \) | Prove \( A \). Then prove \( B \). |
| \( \neg A \) | Simplify the negation, then consult this table on the result. |
To *prove* that this is true...

<table>
<thead>
<tr>
<th><strong>∀x. A</strong></th>
<th>Have the reader pick an arbitrary x. We then prove A is true for that choice of x.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>∃x. A</strong></td>
<td>Find an x where A is true. Then prove that A is true for that specific choice of x.</td>
</tr>
<tr>
<td><strong>A → B</strong></td>
<td>Assume A is true, then prove B is true.</td>
</tr>
<tr>
<td><strong>A ∧ B</strong></td>
<td>Prove A. Then prove B.</td>
</tr>
<tr>
<td><strong>A ∨ B</strong></td>
<td>Either prove ¬A → B or prove ¬B → A. <em>(Why does this work?)</em></td>
</tr>
<tr>
<td><strong>A ↔ B</strong></td>
<td>Prove A → B and B → A.</td>
</tr>
<tr>
<td><strong>¬A</strong></td>
<td>Simplify the negation, then consult this table on the result.</td>
</tr>
</tbody>
</table>
Another Class of Functions
Surjective Functions

• A function \( f : A \rightarrow B \) is called **surjective** (or **onto**) if this first-order logic statement is true about \( f \):

\[
\forall b \in B. \exists a \in A. f(a) = b
\]

(“For every output, there's an input that produces it.”)

• A function with this property is called a **surjection**.

• How does this compare to our first rule of functions?
Theorem: Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.
Surjective Functions

**Theorem:** Let \( f : \mathbb{R} \rightarrow \mathbb{R} \) be defined as \( f(x) = 2x \). Then \( f(x) \) is surjective.

**Proof:**
Surjective Functions

**Theorem:** Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

**Proof:**

What does it mean for $f$ to be surjective?

$$\forall y \in \mathbb{R}. \exists x \in \mathbb{R}. f(x) = y$$

Therefore, we'll choose an arbitrary $y \in \mathbb{R}$, then prove that there is some $x \in \mathbb{R}$ where $f(x) = y$. 

Theorem: Let \( f : \mathbb{R} \to \mathbb{R} \) be defined as \( f(x) = 2x \). Then \( f(x) \) is surjective.

Proof:

What does it mean for \( f \) to be surjective?

\[ \forall y \in \mathbb{R}. \exists x \in \mathbb{R}. f(x) = y \]

Therefore, we'll choose an arbitrary \( y \in \mathbb{R} \), then prove that there is some \( x \in \mathbb{R} \) where \( f(x) = y \).
Surjective Functions

**Theorem:** Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

**Proof:**

What does it mean for $f$ to be surjective?

$$\forall y \in \mathbb{R}. \exists x \in \mathbb{R}. f(x) = y$$

Therefore, we'll choose an arbitrary $y \in \mathbb{R}$, then prove that there is some $x \in \mathbb{R}$ where $f(x) = y$. 

$$x = \frac{y}{2}$$

Then $f(x) = f\left(\frac{y}{2}\right) = 2 \left(\frac{y}{2}\right) = y$. So $f(x) = y$, as required. ■
Theorem: Let \( f : \mathbb{R} \rightarrow \mathbb{R} \) be defined as \( f(x) = 2x \). Then \( f(x) \) is surjective.

Proof:

What does it mean for \( f \) to be surjective?

\[ \forall y \in \mathbb{R}. \exists x \in \mathbb{R}. \; f(x) = y \]

Therefore, we'll choose an arbitrary \( y \in \mathbb{R} \), then prove that there is some \( x \in \mathbb{R} \) where \( f(x) = y \).
Surjective Functions

**Theorem:** Let \( f : \mathbb{R} \to \mathbb{R} \) be defined as \( f(x) = 2x \). Then \( f(x) \) is surjective.

**Proof:**
**Theorem:** Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

**Proof:** Consider any $y \in \mathbb{R}$. Let $x = y/2$. Then we see that $f(x) = f(y/2) = 2y/2 = y$. So $f(x) = y$, as required. ■


**Theorem:** Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

**Proof:** Consider any $y \in \mathbb{R}$. We will prove that there is a choice of $x \in \mathbb{R}$ such that $f(x) = y$. Let $x = y/2$. Then we see that $f(x) = f(y/2) = 2y/2 = y$. So $f(x) = y$, as required. ■
Surjective Functions

**Theorem:** Let \( f : \mathbb{R} \to \mathbb{R} \) be defined as \( f(x) = 2x \). Then \( f(x) \) is surjective.

**Proof:** Consider any \( y \in \mathbb{R} \). We will prove that there is a choice of \( x \in \mathbb{R} \) such that \( f(x) = y \).

Let \( x = y / 2 \).
**Theorem:** Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

**Proof:** Consider any $y \in \mathbb{R}$. We will prove that there is a choice of $x \in \mathbb{R}$ such that $f(x) = y$.

Let $x = y / 2$. Then we see that

$$f(x) = f(y / 2)$$
Surjective Functions

**Theorem:** Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

**Proof:** Consider any $y \in \mathbb{R}$. We will prove that there is a choice of $x \in \mathbb{R}$ such that $f(x) = y$.

Let $x = y / 2$. Then we see that

$$f(x) = f(y / 2) = 2y / 2$$
Surjective Functions

**Theorem:** Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

**Proof:** Consider any $y \in \mathbb{R}$. We will prove that there is a choice of $x \in \mathbb{R}$ such that $f(x) = y$.

Let $x = y / 2$. Then we see that

$$f(x) = f(y / 2) = 2y / 2 = y.$$
Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

Proof: Consider any $y \in \mathbb{R}$. We will prove that there is a choice of $x \in \mathbb{R}$ such that $f(x) = y$.

Let $x = y / 2$. Then we see that

$$f(x) = f(y / 2) = 2y / 2 = y.$$ 

So $f(x) = y$, as required.
Surjective Functions

**Theorem:** Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

**Proof:** Consider any $y \in \mathbb{R}$. We will prove that there is a choice of $x \in \mathbb{R}$ such that $f(x) = y$.

Let $x = y / 2$. Then we see that

$$f(x) = f(y / 2) = 2y / 2 = y.$$ 

So $f(x) = y$, as required. ■
Theorem: Let $g : \mathbb{N} \to \mathbb{N}$ be defined as $g(n) = 2n$. Then $g(x)$ is not surjective.
Surjective Functions

**Theorem:** Let \( g : \mathbb{N} \rightarrow \mathbb{N} \) be defined as \( g(n) = 2n \). Then \( g(x) \) is not surjective.

What does it mean for \( g \) to be surjective?

\[
\forall n \in \mathbb{N}. \exists m \in \mathbb{N}. g(m) = n
\]

What is the negation of the above statement?

\[
\neg \forall n \in \mathbb{N}. \exists m \in \mathbb{N}. g(m) = n \\
\exists n \in \mathbb{N}. \neg \exists m \in \mathbb{N}. g(m) = n \\
\exists n \in \mathbb{N}. \forall m \in \mathbb{N}. g(m) \neq n
\]

Therefore, we need to find a natural number \( n \) where, regardless of which \( m \) we pick, we have \( g(m) \neq n \).
**Theorem:** Let $g : \mathbb{N} \rightarrow \mathbb{N}$ be defined as $g(n) = 2n$. Then $g(x)$ is not surjective.

**Proof:**
Surjective Functions

**Theorem:** Let \( g : \mathbb{N} \to \mathbb{N} \) be defined as \( g(n) = 2n \). Then \( g(x) \) is not surjective.

**Proof:** Let \( n = 137 \).
Surjective Functions

**Theorem:** Let $g : \mathbb{N} \to \mathbb{N}$ be defined as $g(n) = 2n$. Then $g(x)$ is not surjective.

**Proof:** Let $n = 137$.

Our overall goal is to prove

$$\exists n \in \mathbb{N}. \forall m \in \mathbb{N}. g(m) \neq n.$$ 

We just made our choice of $n$. Therefore, we need to prove

$$\forall m \in \mathbb{N}. g(m) \neq n.$$ 

We’ll therefore pick an arbitrary $m \in \mathbb{N}$, then prove that $g(m) \neq n$. 
Surjective Functions

**Theorem:** Let \( g : \mathbb{N} \rightarrow \mathbb{N} \) be defined as \( g(n) = 2n \). Then \( g(x) \) is not surjective.

**Proof:** Let \( n = 137 \). Now, pick an arbitrary \( m \in \mathbb{N} \).
Surjective Functions

**Theorem:** Let $g : \mathbb{N} \rightarrow \mathbb{N}$ be defined as $g(n) = 2n$. Then $g(x)$ is not surjective.

**Proof:** Let $n = 137$. Now, pick an arbitrary $m \in \mathbb{N}$. We need to show that $g(m) \neq n$. Notice that $g(m) = 2m$ is even, while 137 is odd. Therefore, we have $g(m) \neq 137$, as required. □
Theorem: Let $g : \mathbb{N} \rightarrow \mathbb{N}$ be defined as $g(n) = 2n$. Then $g(x)$ is not surjective.

Proof: Let $n = 137$. Now, pick an arbitrary $m \in \mathbb{N}$. We need to show that $g(m) \neq n$.

Notice that $g(m) = 2m$ is even, while 137 is odd.
**Theorem:** Let $g : \mathbb{N} \rightarrow \mathbb{N}$ be defined as $g(n) = 2n$. Then $g(x)$ is not surjective.

**Proof:** Let $n = 137$. Now, pick an arbitrary $m \in \mathbb{N}$. We need to show that $g(m) \neq n$.

Notice that $g(m) = 2m$ is even, while 137 is odd. Therefore, we have $g(m) \neq 137$, as required.
Theorem: Let \( g : \mathbb{N} \to \mathbb{N} \) be defined as \( g(n) = 2n \). Then \( g(x) \) is not surjective.

Proof: Let \( n = 137 \). Now, pick an arbitrary \( m \in \mathbb{N} \). We need to show that \( g(m) \neq n \).

Notice that \( g(m) = 2m \) is even, while 137 is odd. Therefore, we have \( g(m) \neq 137 \), as required. \( \blacksquare \)
Surjective Functions

**Theorem:** Let \( g : \mathbb{N} \rightarrow \mathbb{N} \) be defined as \( g(n) = 2n \). Then \( g(x) \) is not surjective.

**Proof:** Let \( n = 137 \). Now, pick an arbitrary \( m \in \mathbb{N} \). We need to show that \( g(m) \neq n \).

Notice that \( g(m) = 2m \) is even, while 137 is odd. Therefore, we have \( g(m) \neq 137 \), as required. ■
<table>
<thead>
<tr>
<th>Logical Form</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\forall x. A$</td>
<td>Have the reader pick an arbitrary $x$. We then prove $A$ is true for that choice of $x$.</td>
</tr>
<tr>
<td>$\exists x. A$</td>
<td>Find an $x$ where $A$ is true. Then prove that $A$ is true for that specific choice of $x$.</td>
</tr>
<tr>
<td>$A \rightarrow B$</td>
<td>Assume $A$ is true, then prove $B$ is true.</td>
</tr>
<tr>
<td>$A \land B$</td>
<td>Prove $A$. Then prove $B$.</td>
</tr>
<tr>
<td>$A \lor B$</td>
<td>Either prove $\neg A \rightarrow B$ or prove $\neg B \rightarrow A$. <em>(Why does this work?)</em></td>
</tr>
<tr>
<td>$A \leftrightarrow B$</td>
<td>Prove $A \rightarrow B$ and $B \rightarrow A$.</td>
</tr>
<tr>
<td>$\neg A$</td>
<td>Simplify the negation, then consult this table on the result.</td>
</tr>
</tbody>
</table>
Recap from Today

- A **function** takes in an element of a **domain** and maps it to an element of a **codomain**. Functions must be deterministic.

- Definitions are often given in first-order logic, and the structure of a first-order logic statement dictates the structure of a proof.

- **Involutions**, **injections**, and **surjections** are specific classes of functions that have nice properties.
Next Time

- **First-Order Assumptions**
  - The difference between assuming something is true and proving something is true.

- **Connecting Function Types**
  - Involutions, injections, and surjections are related to one another. How?

- **Function Composition**
  - Sequencing functions together.