Functions

Part Two

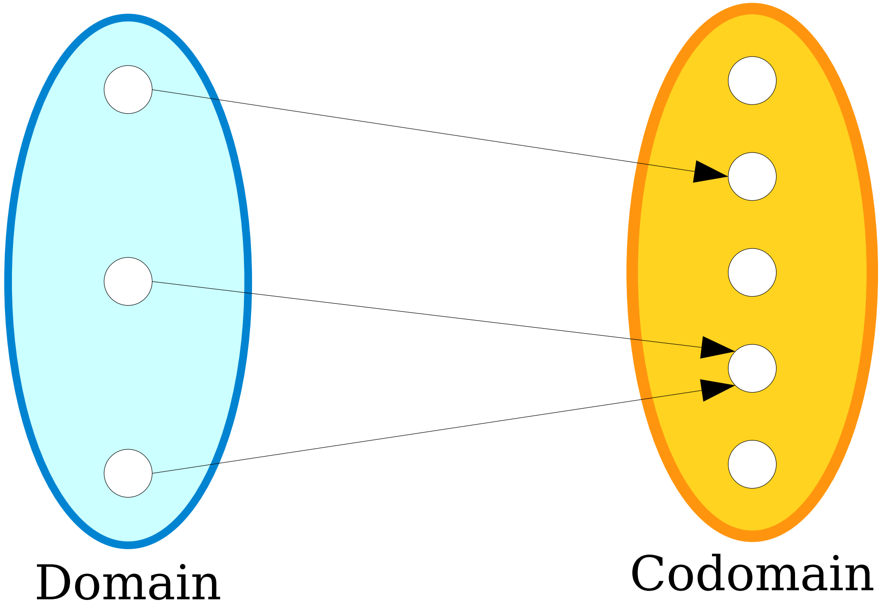
Outline for Today

- ***Recap from Last Time***
  - Where are we, again?
- ***Injections and Surjections***
  - Two useful classes of functions.
- ***A Proof About Birds***
  - Trust me, it's relevant.
- ***Assuming vs Proving***
  - Two different roles to watch for.
- ***Connecting Function Types***
  - Relating the topics from last time.

Recap from Last Time

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.
- We write **$f : A \to B$** to indicate that f is a function whose domain is A and whose codomain is B.



The function must be defined for each element of its domain.

The output of the function must always be in the codomain, but not all elements of the codomain need to be producable.

Involutions

- A function $f : A \to A$ 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.")

- For example, $f : \mathbb{R} \to \mathbb{R}$ defined as $f(x) = -x$ is an involution.

Injective Functions

- A function $f : A \to B$ is called ***injective*** (or ***one-to-one***) if different inputs always map to different outputs.
    - A function with this property is called an ***injection***.
- Formally, $f : A \to B$ is an injection if this FOL statement is true:

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

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

- Equivalently:

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

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

	To ***prove*** that this is true…	
$\forall x.\ A$	Have the reader pick an arbitrary x. 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.	

New Stuff!

Proofs on Injections

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?

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

$$\forall n_1 \in \mathbb{N}.\ \forall n_2 \in \mathbb{N}.\ (\ n_1 \neq n_2 \to f(n_1) \neq f(n_2)\ )$$

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: 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 $f : \mathbb{N} \to \mathbb{N}$ 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. ■

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

Proof:

What does it mean for f to be injective?

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

What is the negation of this statement?

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

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

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

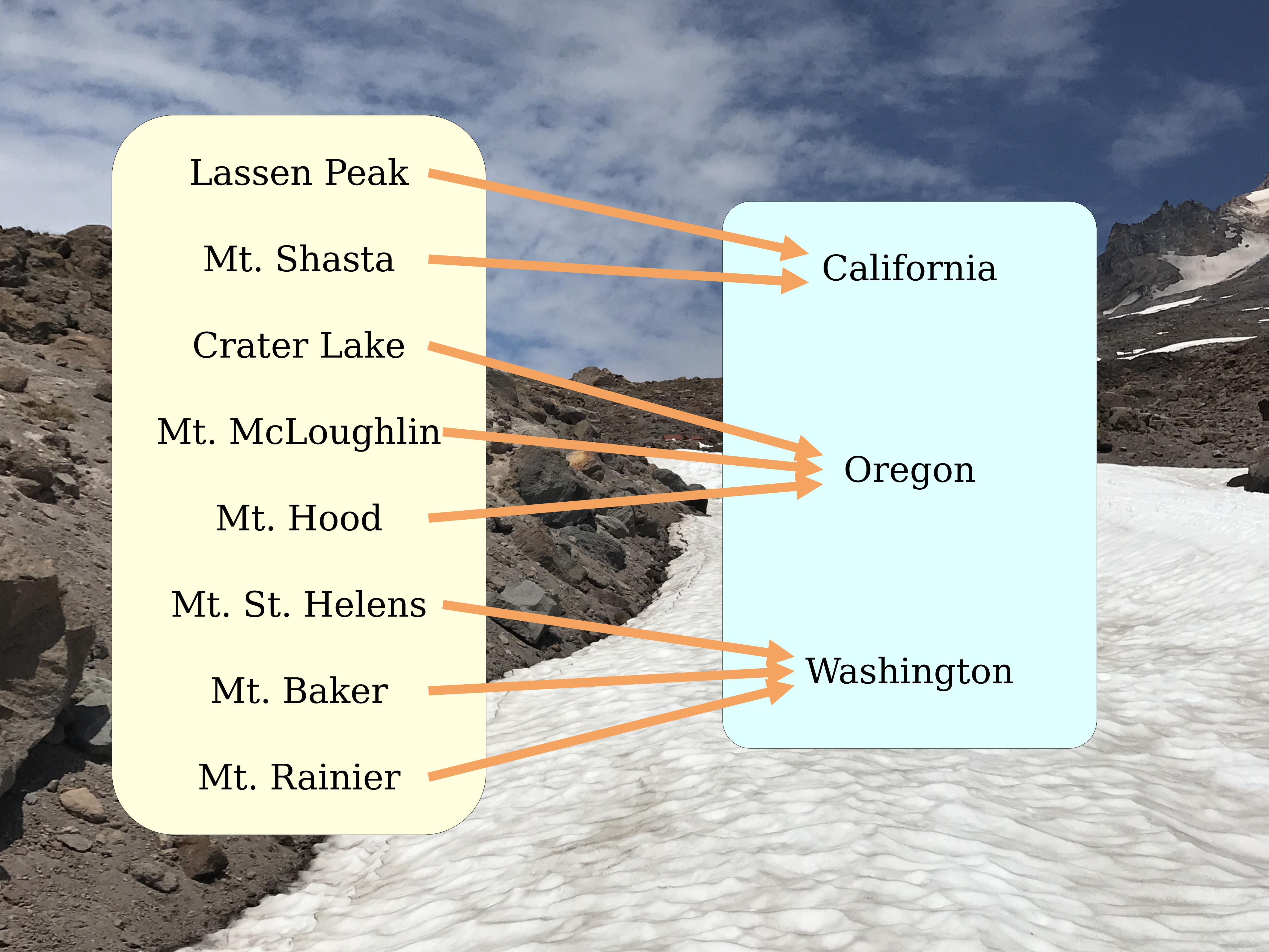
and

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

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

	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.	
$A \to B$	Assume A is true, then prove B is true.	
$A \land B$	Prove A. Then prove B.	
$A \lor B$	Either prove $\neg A \to B$ or prove $\neg B \to A$. *(Why does this work?)*	
$A \leftrightarrow B$	Prove $A \to B$ and $B \to A$.	
$\neg A$	Simplify the negation, then consult this table on the result.	

Another Class of Functions



Lassen Peak

Mt. Shasta

Crater Lake

Mt. McLoughlin

Mt. Hood

Mt. St. Helens

Mt. Baker

Mt. Rainier

California

Oregon

Washington

Surjective Functions

- A function $f : A \to B$ 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?

Check the appendix for sample proofs involving injections.

A Proof About Birds

Theorem: If all birds can fly,
then all herons can fly.

Theorem: If all birds can fly, then all herons can fly.

Given the predicates

$Bird(b)$, which says b is a bird;
$Heron(h)$, which says h is a heron; and
$CanFly(x)$, which says x can fly,

translate the theorem into first-order logic.

$$\underbrace{(\forall b.\ (Bird(b) \to CanFly(b)))}_{\text{All birds can fly}} \to \underbrace{(\forall h.\ (Heron(h) \to CanFly(h)))}_{\text{All herons can fly}}$$

	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.	
$A \to B$	Assume A is true, then prove B is true.	
$A \land B$	Prove A. Then prove B.	
	Either prove $\neg A \to B$ or	

$$\underbrace{(\forall b.\ (Bird(b) \to CanFly(b)))}_{\text{All birds can fly}} \to \underbrace{(\forall h.\ (Heron(h) \to CanFly(h)))}_{\text{All herons can fly}}$$

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

Which makes more sense as the next step in this proof?

1. Consider an arbitrary bird b.
2. Consider an arbitrary heron h.

$$\underbrace{(\forall b.\ (\mathit{Bird}(b) \to \mathit{CanFly}(b)))}_{\text{All birds can fly}} \to \underbrace{(\forall h.\ (\mathit{Heron}(h) \to \mathit{CanFly}(h)))}_{\text{All herons can fly}}$$

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

Consider an arbitrary bird b. Since b is a bird, b can fly. *[and now we're stuck! we are interested in herons, but b might not be one. It could be a hummingbird, for example!]*

$$\underbrace{(\forall b.\ (Bird(b) \to CanFly(b)))}_{\text{All birds can fly}} \to \underbrace{(\forall h.\ (Heron(h) \to CanFly(h)))}_{\text{All herons can fly}}$$

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

Consider an arbitrary heron *h*. We will show that *h* can fly. To do so, note that since *h* is a heron we know *h* is a bird. Therefore, by our earlier assumption, *h* can fly. ■

$$\underbrace{(\forall b.\ (Bird(b) \to CanFly(b)))}_{\text{All birds can fly}} \to \underbrace{(\forall h.\ (Heron(h) \to CanFly(h)))}_{\text{All herons can fly}}$$

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

Consider an arbitrary heron *h*. We will show that *h* can fly. To do so, note that since *h* is a heron we know *h* is a bird. Therefore, by our earlier assumption, *h* can fly. ■

$$\underbrace{(\forall b.\ (Bird(b) \to CanFly(b)))}_{\text{We never introduce a variable } b.} \to \underbrace{(\forall h.\ (Heron(h) \to CanFly(h)))}_{\text{We introduce a variable } h \text{ almost immediately.}}$$

Proving vs. Assuming

- In the context of a proof, you will need to assume some statements and prove others.
  - Here, we ***assumed*** all birds can fly.
  - Here, we ***proved*** all herons can fly.
- Statements behave differently based on whether you're assuming or proving them.

$$\underbrace{(\forall b.\ (\mathit{Bird}(b) \to \mathit{CanFly}(b)))}_{\text{We never introduce a variable } b.} \to \underbrace{(\forall h.\ (\mathit{Heron}(h) \to \mathit{CanFly}(h)))}_{\text{We introduce a variable } h \text{ almost immediately.}}$$

Proving vs. Assuming

- To ***prove*** the universally-quantified statement

  $$\forall x.\ P(x)$$

  we introduce a new variable x representing some arbitrarily-chosen value.
- Then, we prove that $P(x)$ is true for that variable x.
- That's why we introduced a variable h in this proof representing a heron.

$$\underbrace{(\forall b.\ (Bird(b) \to CanFly(b)))}_{\text{We never introduce a variable } b.} \to \underbrace{(\forall h.\ (Heron(h) \to CanFly(h)))}_{\text{We introduce a variable } h \text{ almost immediately.}}$$

Proving vs. Assuming

- If we ***assume*** the statement

  $$\forall x.\ P(x)$$

  we ***do not*** introduce a variable x.
- Rather, if we find a relevant value z somewhere else in the proof, we can conclude that $P(z)$ is true.
- That's why we didn't introduce a variable b in our proof, and why we concluded that h, our heron, can fly.

$$\underbrace{(\forall b.\ (Bird(b) \to CanFly(b)))}_{\text{We never introduce a variable } b.} \to \underbrace{(\forall h.\ (Heron(h) \to CanFly(h)))}_{\text{We introduce a variable } h \text{ almost immediately.}}$$

	To ***prove*** that this is true…	If you ***assume*** this is true…
$\forall x.\ A$	Have the reader pick an arbitrary x. We then prove A is true for that choice of x.	Initially, ***do nothing***. Once you find a z through other means, you can state it has property A.
$\exists x.\ A$	Find an x where A is true. Then prove that A is true for that specific choice of x.	Introduce a variable x into your proof that has property A.
$A \to B$	Assume A is true, then prove B is true.	Initially, ***do nothing***. Once you know A is true, you can conclude B is also true.
$A \land B$	Prove A. Then prove B.	Assume A. Then assume B.
$A \lor B$	Either prove $\neg A \to B$ or prove $\neg B \to A$. *(Why does this work?)*	Consider two cases. Case 1: A is true. Case 2: B is true.
$A \leftrightarrow B$	Prove $A \to B$ and $B \to A$.	Assume $A \to B$ and $B \to A$.
$\neg A$	Simplify the negation, then consult this table on the result.	Simplify the negation, then consult this table on the result.

Connecting Function Types

Types of Functions

- We now have three special types of functions:
  - ***involutions***, functions that undo themselves;
  - ***injections***, functions where different inputs go to different outputs; and
  - ***surjections***, functions that cover their whole codomain.
- ***Question:*** How do these three classes of functions relate to one another?

Theorem: For any function $f : A \to A$,
if f is an involution, then f is surjective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{f \text{ is an involution.}} \quad \to \quad \underbrace{(\forall b \in A.\ \exists a \in A.\ f(a) = b)}_{f \text{ is surjective.}}$$

Theorem: For any function $f : A \to A$,
if f is an involution, then f is surjective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{\text{Assume this.}} \quad \to \quad \underbrace{(\forall b \in A.\ \exists a \in A.\ f(a) = b)}_{\text{Prove this.}}$$

Theorem: For any function $f : A \to A$,
if f is an involution, then f is surjective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{\text{Assume this.}} \rightarrow \underbrace{(\forall b \in A.\ \exists a \in A.\ f(a) = b)}_{\text{Prove this.}}$$

$$\boxed{\underbrace{(\forall b.\ (Bird(b) \rightarrow CanFly(b)))}_{\text{Assume this.}} \rightarrow \underbrace{(\forall h.\ (Heron(h) \rightarrow CanFly(h)))}_{\text{Prove this.}}}$$

Theorem: For any function $f : A \rightarrow A$,
if f is an involution, then f is surjective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{\text{Assume this.}} \to \underbrace{(\forall b \in A.\ \exists a \in A.\ f(a) = b)}_{\text{Prove this.}}$$

If you ***assume***
this is true…

Initially, ***do nothing***. Once you find a z through other means, you can state it has property A.

Theorem: For any function $f : A \to A$,
if f is an involution, then f is surjective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)} \to \underbrace{(\forall b \in A.\ \exists a \in A.\ f(a) = b)}$$

Assume this.

Prove this.

Since we're *assuming* this, we aren't going to pick a specific choice of x right now. Instead, we're going to keep an eye out for something to apply this fact to.

Proof Outline

1. Assume f is an involution.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{\text{Ass}} \to \underbrace{(\forall b \in A.\ \exists a \in A.\ f(a) = b)}_{\text{Prove this.}}$$

We've said that we need to *prove* this statement. How do we do that?

Proof Outline

1. Assume f is an involution.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{\text{Assume this.}} \to \underbrace{(\forall b \in A.\ \exists a \in A.\ f(a) = b)}_{\text{Prove this.}}$$

To ***prove*** that this is true…

Have the reader pick an arbitrary x. Then prove A is true for that choice of x.

Proof Outline

1. Assume f is an involution.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{\text{Ass}} \to \underbrace{(\forall b \in A.\ \exists a \in A.\ f(a) = b)}_{\text{Prove this.}}$$

There's a universal quantifier up front. Since we're *proving* this, we'll pick an arbitrary $b \in A$.

Proof Outline

1. Assume f is an involution.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{\text{Ass}} \to \underbrace{(\forall b \in A.\ \exists a \in A.\ f(a) = b)}_{\text{Prove this.}}$$

There's a universal quantifier up front. Since we're *proving* this, we'll pick an arbitrary $b \in A$.

Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

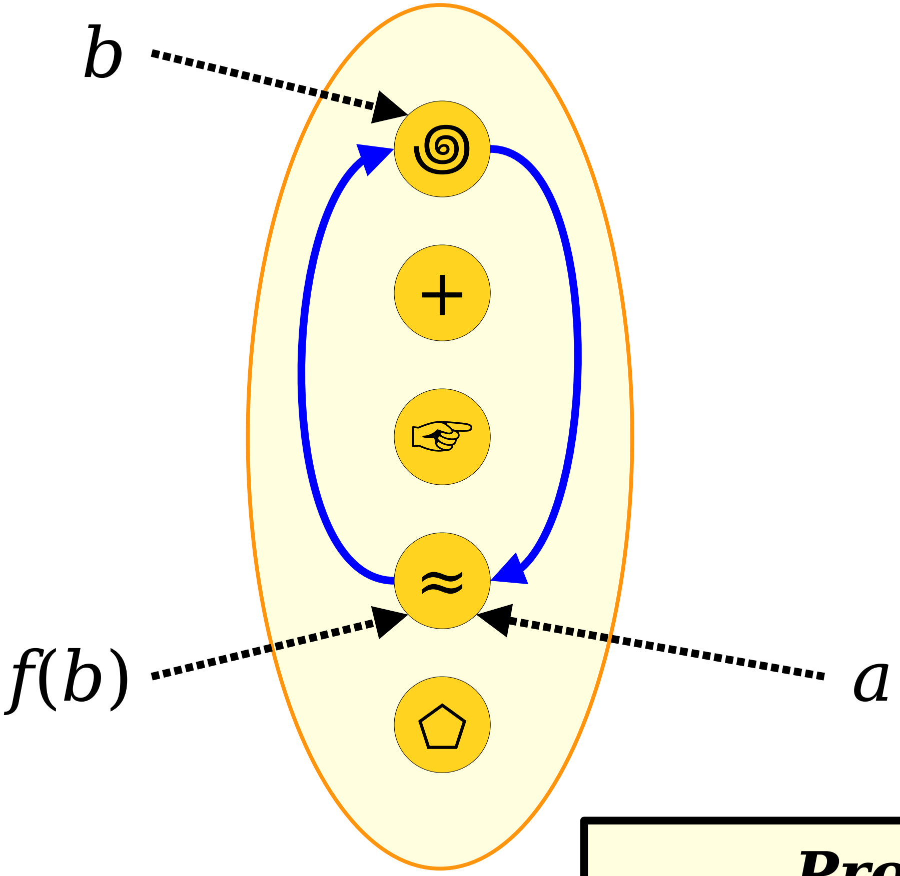
$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{} \quad \to \quad \underbrace{(\forall b \in A.\ \exists a \in A.\ f(a) = b)}_{\text{Prove this.}}$$

Now, we hit an existential quantifier. Since we're *proving* this, we need to find a choice of $a \in A$ where this is true.

Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.
3. Give a choice of $a \in A$ where $f(a) = b$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.



Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.
3. Give a choice of $a \in A$ where $f(a) = b$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

Proof: Pick any involution $f : A \to A$. We will prove that f is surjective. To do so, pick an arbitrary $b \in A$. We need to show that there is an $a \in A$ where $f(a) = b$.

Specifically, pick $a = f(b)$. This means that $f(a) = f(f(b))$, and since f is an involution we know that $f(f(b)) = b$. Putting this together, we see that $f(a) = b$, which is what we needed to show. ■

Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.
3. Give a choice of $a \in A$ where $f(a) = b$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

Proof: Pick any involution $f : A \to A$. We will prove that f is surjective. To do so, pick an arbitrary $b \in A$. We need to show that there is an $a \in A$ where $f(a) = b$.

Specifically, pick $a = f(b)$. This means that $f(a) = f(f(b))$, and since f is an involution we know that $f(f(b)) = b$. Putting this together, we see that $f(a) = b$, which is what we needed to show. ■

This proof contains no first-order logic syntax (quantifiers, connectives, etc.). It's written in plain English, just as usual.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

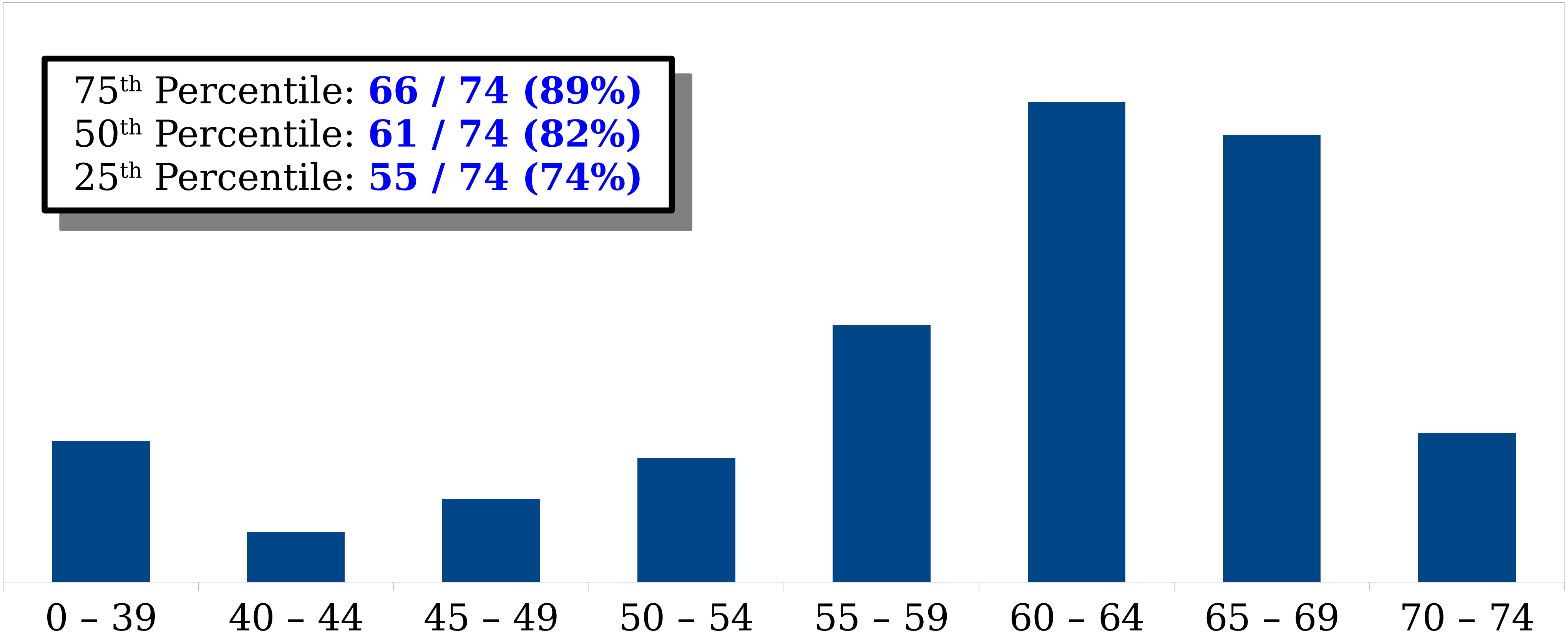
Proof: In the slide appendix!

Time-Out for Announcements!

Problem Set One Graded

- Your wonderful TAs have finished grading Problem Set One.
- Grades and feedback are up on the Gradescope.
- Solutions are available online on the course website (visit the page for PS1 to get the link).

Problem Set One Graded

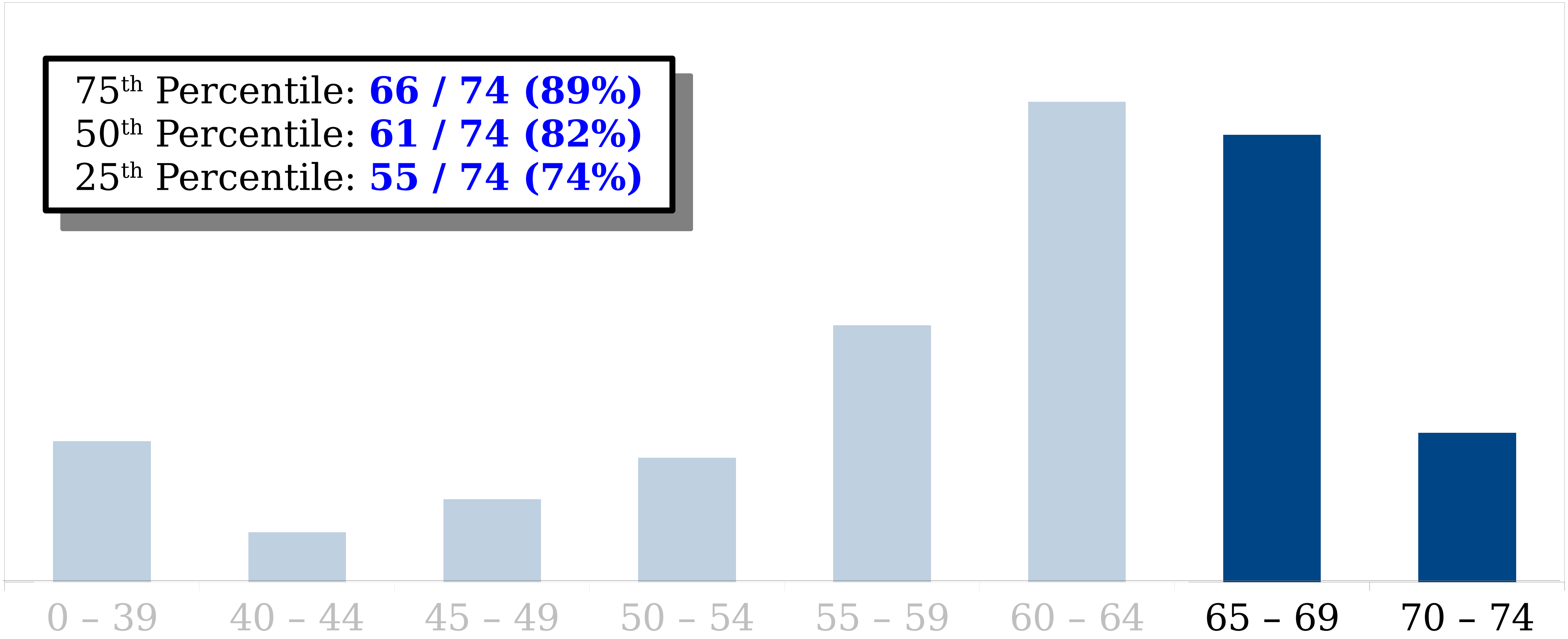


75th Percentile: **66 / 74 (89%)**
50th Percentile: **61 / 74 (82%)**
25th Percentile: **55 / 74 (74%)**

Pro tips when reading a grading distribution:

1. Standard deviations are ***unhelpful and discouraging***. Ignore them.
2. The average score is a ***unhelpful***. Ignore it.
3. Raw scores are ***unhelpful and discouraging***. Ignore them.

Problem Set One Graded

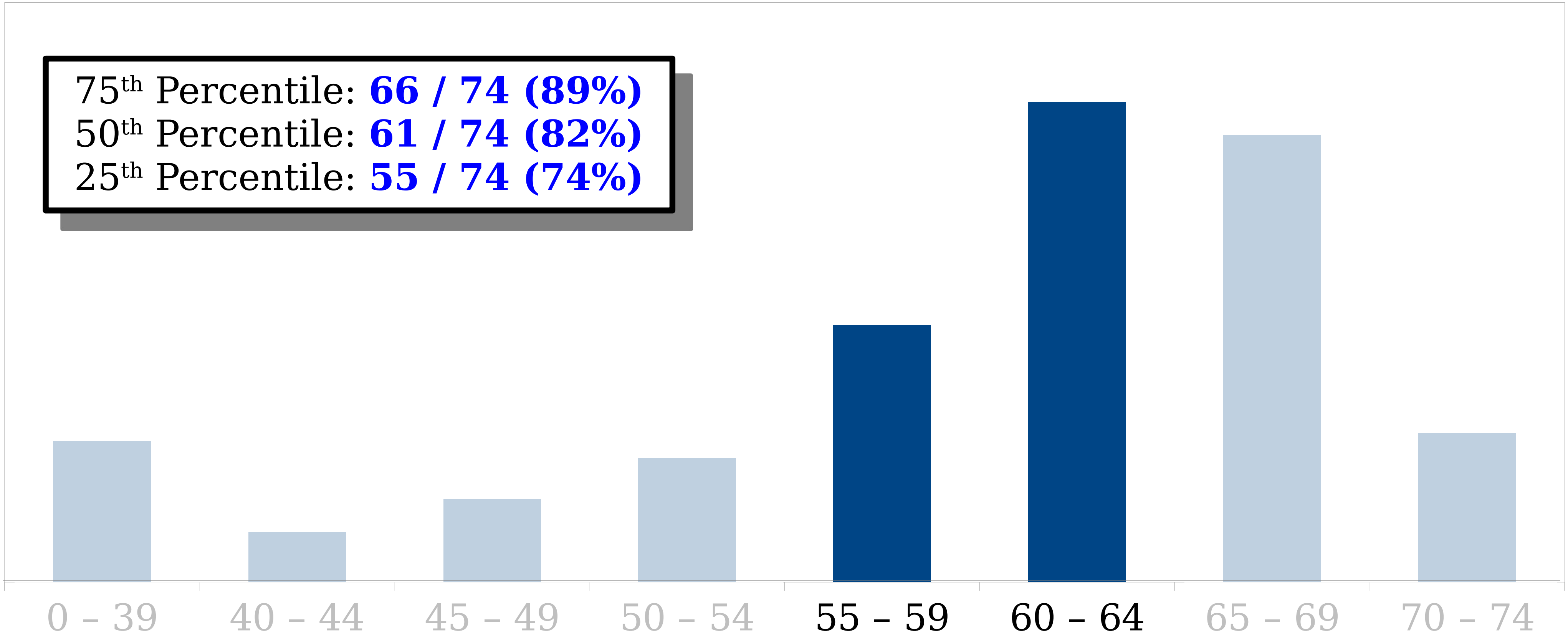


75th Percentile: **66 / 74 (89%)**
50th Percentile: **61 / 74 (82%)**
25th Percentile: **55 / 74 (74%)**

"Great job! Look over your feedback for some tips on how to tweak things for next time."

Problem Set One Graded

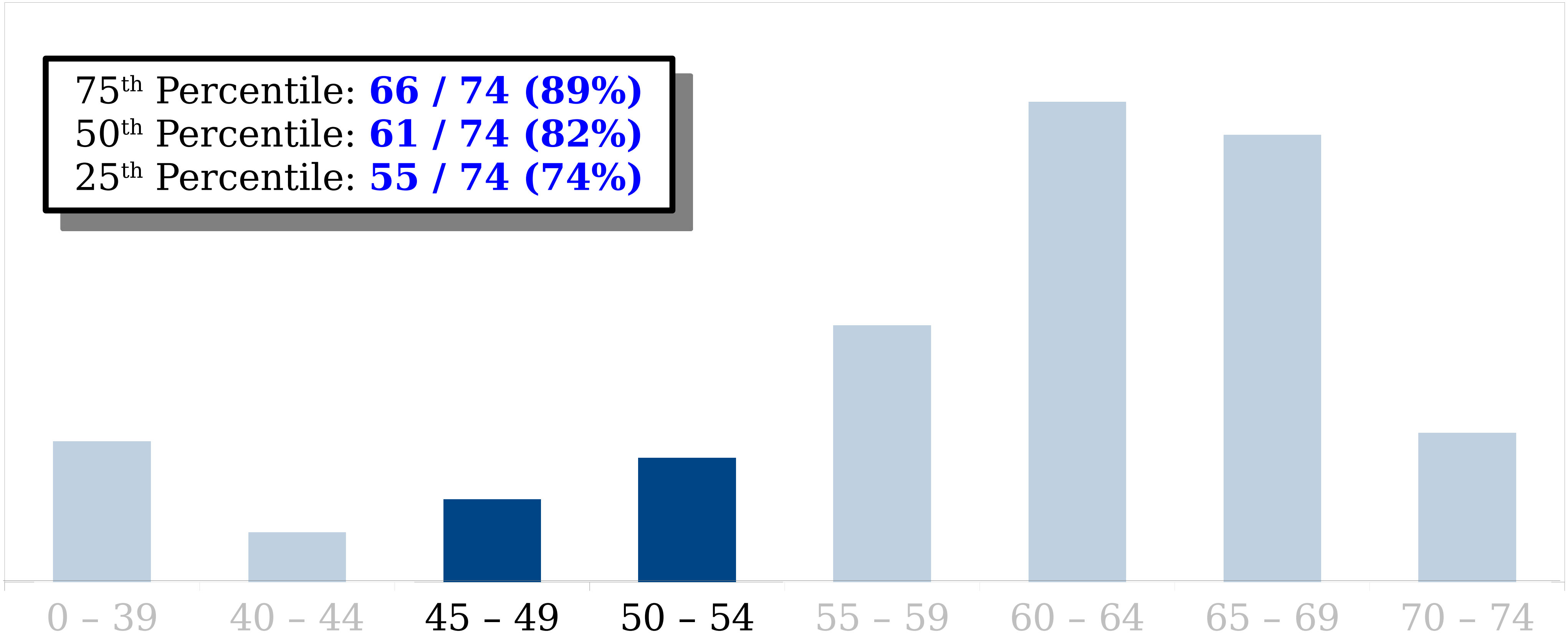
75th Percentile: **66 / 74 (89%)**
50th Percentile: **61 / 74 (82%)**
25th Percentile: **55 / 74 (74%)**



"You're almost there! Review the feedback on your submission and see what to focus on for next time."

Problem Set One Graded

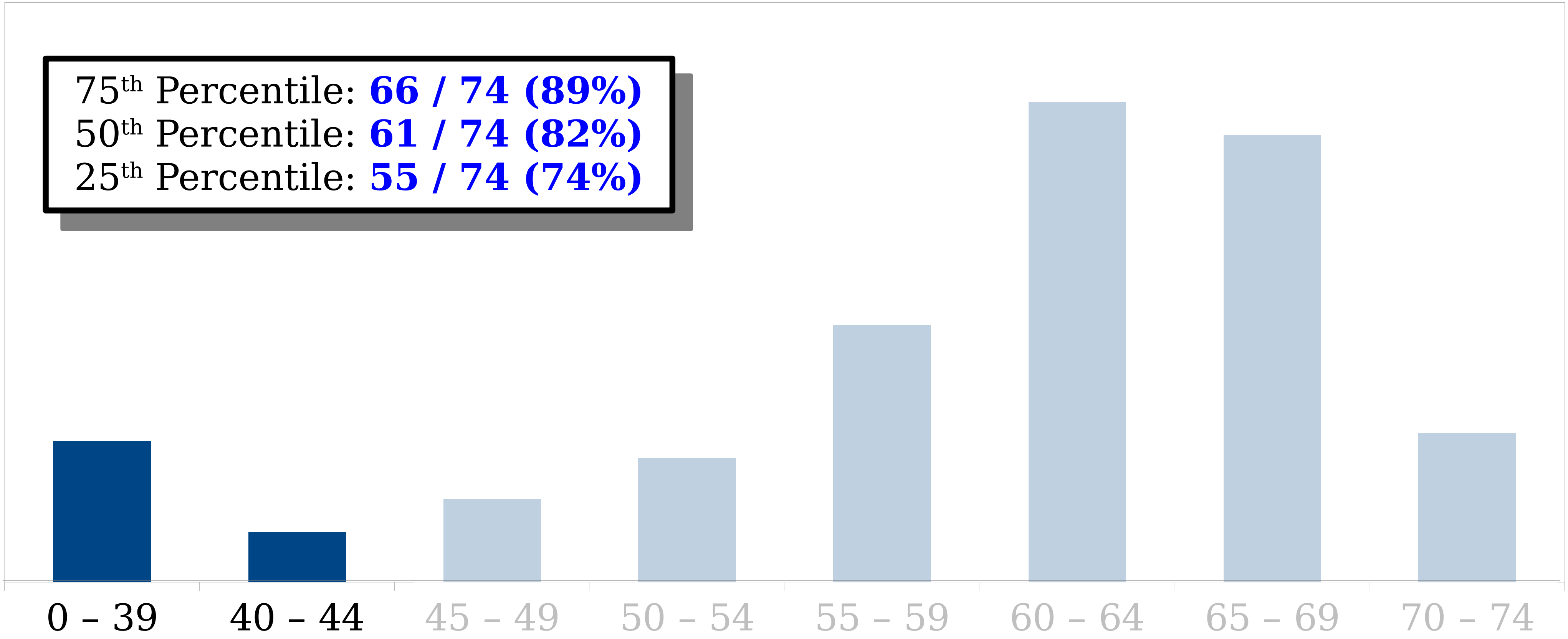
75th Percentile: **66 / 74 (89%)**
50th Percentile: **61 / 74 (82%)**
25th Percentile: **55 / 74 (74%)**



"You're on the right track, but there are some areas where you need to improve. Review your feedback and ask us questions when you have them."

Problem Set One Graded

75th Percentile: **66 / 74 (89%)**
50th Percentile: **61 / 74 (82%)**
25th Percentile: **55 / 74 (74%)**



"Looks like something hasn't quite clicked yet. Get in touch with us and stop by office hours to get some extra feedback and advice. Don't get discouraged – you can do this!"

What Not to Think

- “Well, I guess I’m just not good at math.”
  - For most of you, this is your first time doing any rigorous proof-based math.
  - Don’t judge your future performance based on a single data point.
  - Life advice: think about download times.
  - Life advice: have a growth mindset!
- “Hey, I did above the median. That’s good enough.”
  - There’s always some area where you can improve. Take the time to see what that is.

Regrade Requests

- We’re human. We make mistakes. And we’re happy to correct them!
- Regrades will open on Gradescope 48 hours after grades are released. They close one week after grades are released.
- Notes on regrades:
    - Please be civil. We make mistakes. We’re happy to correct them.
    - We have to grade what you submitted; we can’t take any clarifications into account during regrades.
    - Regrades are for where we made deductions we shouldn’t have, rather than for the magnitude of deductions.

Your Questions

“How are concepts we learn in CS103 applicable to fields outside of CS and math, such as physics, chemistry, or materials science?”

Functions that are both injective and surjective (bijections – a term we'll see Friday) are useful tools in pinning down what symmetry means. That has applications throughout a bunch of other fields, especially physics and MatSci.

Graphs, which we'll cover next week, are indispensable tools in a bunch of different disciplines. They're used to model discrete lattice structures in physics, molecules in chemistry, etc.

Even the limits of computation have applications in the sciences. It's not computationally possible to determine how arbitrary crystals assemble, nor can we determine some physical properties of quantum systems with computers.

Complexity theory is particularly relevant in many disciplines, as some problems that seem easy to state are computationally hard to solve. This dictates what sorts of questions folks then ask.

Major Ideas From Today

- Proofs involving first-order definitions are heavily based on the structure of those definitions, yet FOL notation itself does *not* appear in the proof.
- Statements behave differently based on whether you're ***assuming*** or ***proving*** them.
- When you ***assume*** a universally-quantified statement, initially, do nothing. Instead, keep an eye out for a place to apply the statement more specifically.
- When you ***prove*** a universally-quantified statement, pick an arbitrary value and try to prove it has the needed property.

	To ***prove*** that this is true…	If you ***assume*** this is true…
$\forall x.\ A$	Have the reader pick an arbitrary x. We then prove A is true for that choice of x.	Initially, ***do nothing***. Once you find a z through other means, you can state it has property A.
$\exists x.\ A$	Find an x where A is true. Then prove that A is true for that specific choice of x.	Introduce a variable x into your proof that has property A.
$A \to B$	Assume A is true, then prove B is true.	Initially, ***do nothing***. Once you know A is true, you can conclude B is also true.
$A \land B$	Prove A. Then prove B.	Assume A. Then assume B.
$A \lor B$	Either prove $\neg A \to B$ or prove $\neg B \to A$. *(Why does this work?)*	Consider two cases. Case 1: A is true. Case 2: B is true.
$A \leftrightarrow B$	Prove $A \to B$ and $B \to A$.	Assume $A \to B$ and $B \to A$.
$\neg A$	Simplify the negation, then consult this table on the result.	Simplify the negation, then consult this table on the result.

Next Time

- ***Cardinality Revisited***
  - Formalizing our definitions.
- ***The Nature of Infinity***
  - Infinity is more interesting than it looks!
- ***Cantor's Theorem Revisited***
  - Formally proving a major result.

Appendix: More Proofs on Functions

Proof 1: Proving a function is surjective.

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 $f(x) = y$.

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

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

So $f(x) = y$, as required. ■

This proof contains no first-order logic syntax (quantifiers, connectives, etc.). It's written in plain English, just as usual.

Proof 2: Proving a function is not surjective.

Surjective Functions

Theorem: Let $g : \mathbb{N} \to \mathbb{N}$ 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 $g(m) \neq n$.

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 $g : \mathbb{N} \to \mathbb{N}$ 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. ■

This proof contains no first-order logic syntax (quantifiers, connectives, etc.). It's written in plain English, just as usual.

Proof 3: Proving all involutions are injective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{\substack{f \text{ is an} \\ \text{involution.}}} \rightarrow \underbrace{(\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \rightarrow f(a_1) \neq f(a_2)))}_{\substack{f \text{ is} \\ \text{injective.}}}$$

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{\text{Assume this.}} \to \underbrace{(\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to f(a_1) \neq f(a_2)))}_{\text{Prove this.}}$$

Theorem: For any function $f : A \to A$,
if f is an involution, then f is injective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{\text{Assume this.}} \to \underbrace{(\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to f(a_1) \neq f(a_2)))}_{\text{Prove this.}}$$

$$\boxed{\underbrace{(\forall b.\ (Bird(b) \to CanFly(b)))}_{\text{Assume this.}} \to \underbrace{(\forall h.\ (Heron(h) \to CanFly(h)))}_{\text{Prove this.}}}$$

Theorem: For any function $f : A \to A$,
if f is an involution, then f is injective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{\text{Assume this.}} \to \underbrace{(\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to f(a_1) \neq f(a_2)))}_{\text{Prove this.}}$$

Since we're assuming this, we aren't going to pick a specific choice of x right now. Instead, we're going to keep an eye out for something to apply this fact to.

Proof Outline

1. Assume f is an involution.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}\ \to\ \underbrace{(\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to f(a_1) \neq f(a_2)))}$$

We need to *prove* this part.
What does that mean?

Prove
this.

Proof Outline

1. Assume f is an involution.

Theorem: For any function $f : A \to A$,
if f is an involution, then f is injective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)} \to \underbrace{(\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to f(a_1) \neq f(a_2)))}$$

Since we're *proving* something universally-quantified, we'll pick some values arbitrarily.

Prove this.

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary a_1, $a_2 \in A$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{} \to \underbrace{(\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to f(a_1) \neq f(a_2)))}_{\text{Prove this.}}$$

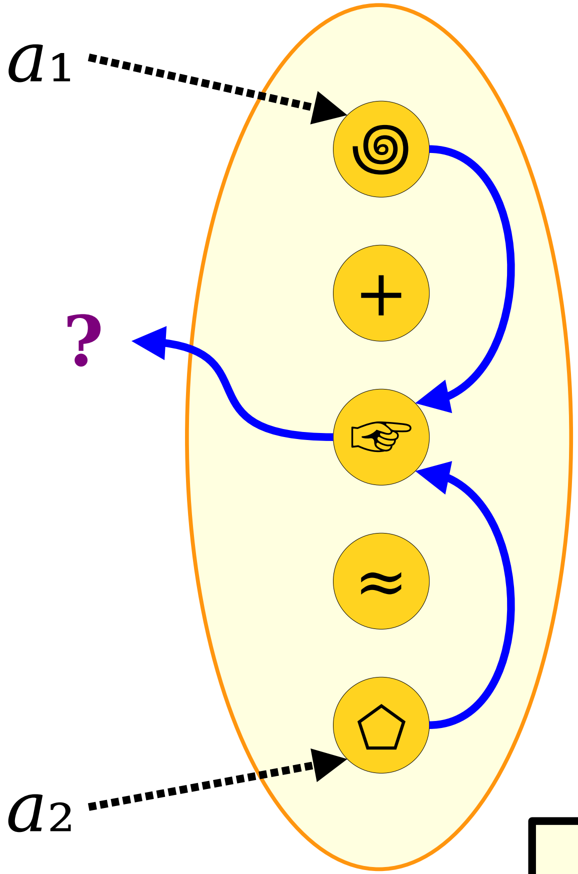
We now need to *prove* this implication. But we know how to do that! We assume the antecedent and prove the consequent.

Prove this.

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.



Proof Outline

1. Assume f is an involution.
2. Pick arbitrary a_1, $a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

Proof: Consider any function $f : A \to A$ that's an involution. We will prove that f is injective. To do so, choose any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We need to show that $f(a_1) \neq f(a_2)$.

We'll proceed by contradiction. Suppose that $f(a_1) = f(a_2)$. This means $f(f(a_1)) = f(f(a_2))$, which in turn tells us $a_1 = a_2$ because f is an involution. But that's impossible, since $a_1 \neq a_2$.

We've reached a contradiction, so our assumption was wrong. Therefore, we see that $f(a_1) \neq f(a_2)$, as required. ■

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.