Functions

Part Two

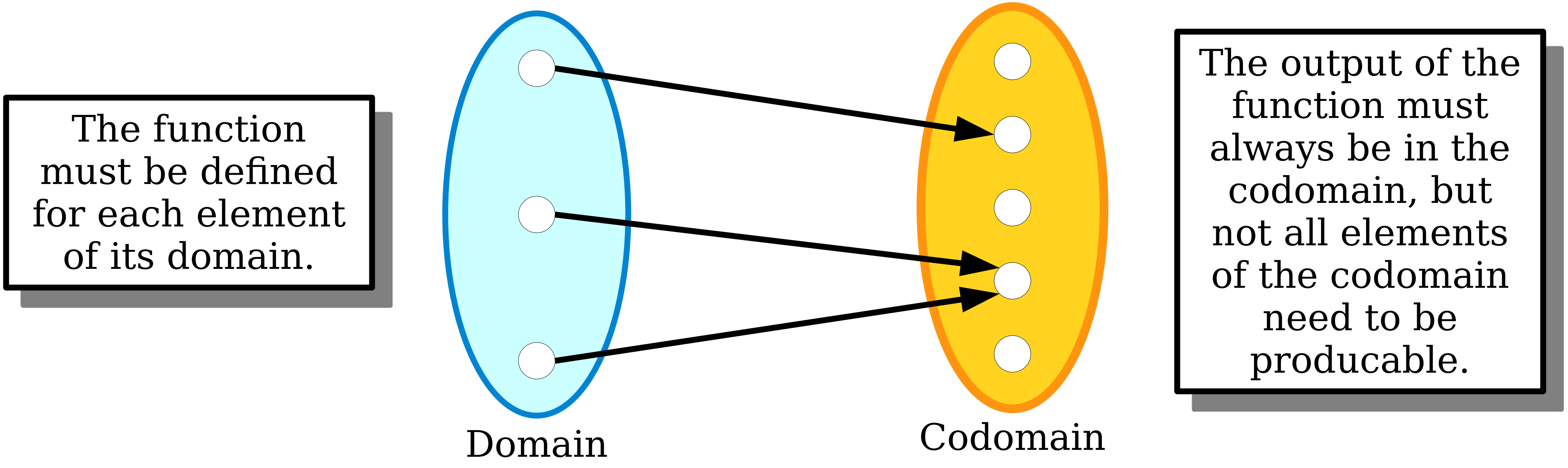
Outline for Today

- ***Recap from Last Time***
  - Where are we, again?
- ***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 $\boldsymbol{f : A \to B}$ to indicate that *f* is a function whose domain is *A* and whose codomain is *B*.



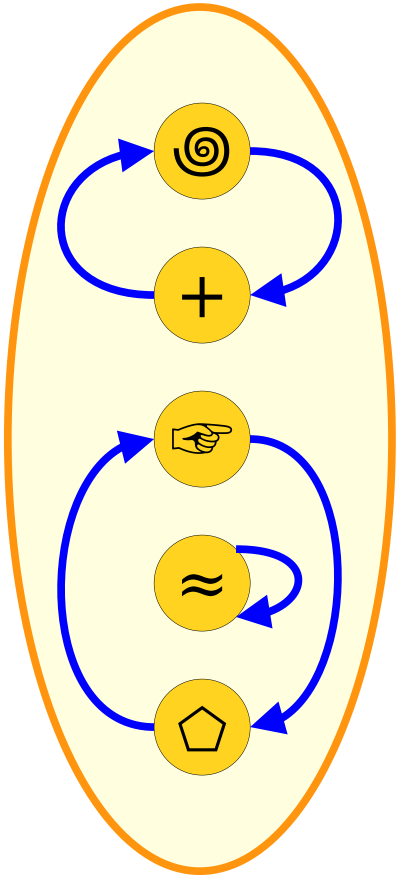
Involutions

- A function $f : A \to A$ from a set back to itself is called an ***involution*** when 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***) when different inputs always map to different outputs.
  - A function with this property is called an ***injection***.
- Formally, $f : A \to B$ is an injection when this FOL statement is true:

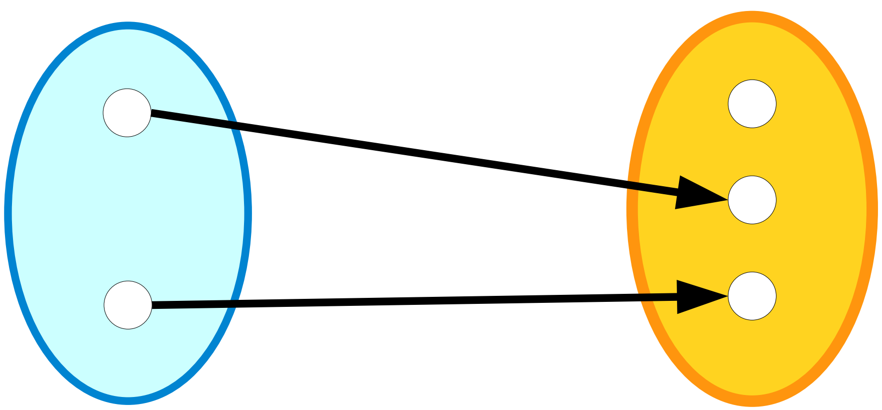
$$\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to f(a_1) \neq f(a_2))$$

(*"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"*)



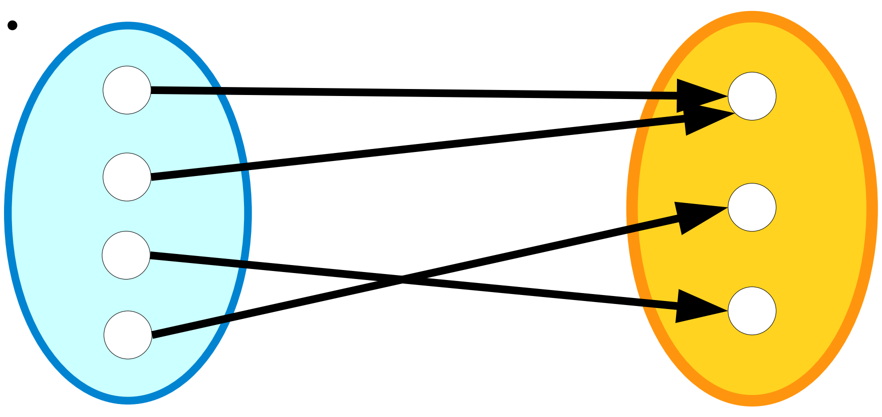
Surjective Functions

- A function $f : A \to B$ is called ***surjective*** (or ***onto***) when this first-order logic statement is true about f:

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

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

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



		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. Also 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.

New Stuff!

A Proof About Birds



Theorem: If all birds have feathers,
then all herons have feathers.

Theorem: If all birds have feathers, then all herons have feathers.

Given the predicates

> $Bird(b)$, which says b is a bird;
> $Heron(h)$, which says h is a heron; and
> $Feathers(x)$, which says x has feathers,

translate the theorem into first-order logic.

$$\underbrace{\left(\forall b.\ (Bird(b) \to Feathers(b))\right)}_{\text{All birds have feathers}} \to \underbrace{\left(\forall h.\ (Heron(h) \to Feathers(h))\right)}_{\text{All herons have feathers}}$$

		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. Also prove B.
		Either prove $\neg A \to B$ or

$$\underbrace{(\forall b.\ (Bird(b) \to Feathers(b)))}_{\text{All birds have feathers}} \to \underbrace{(\forall h.\ (Heron(h) \to Feathers(h)))}_{\text{All herons have feathers}}$$

Theorem: If all birds have feathers, then all herons have feathers.

Proof: Assume that all birds have feathers. We will show that all herons have feathers.

Answer at

https://cs103.stanford.edu/pollev

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

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

$$(\forall b.\ (Bird(b) \to Feathers(b))) \to (\forall h.\ (Heron(h) \to Feathers(h)))$$

All birds have feathers

All herons have feathers

Theorem: If all birds have feathers, then all herons have feathers.

Proof: Assume that all birds have feathers. We will show that all herons have feathers.

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

$$(\forall b.\ (Bird(b) \to Feathers(b))) \to (\forall h.\ (Heron(h) \to Feathers(h)))$$

All birds have feathers

All herons have feathers

Theorem: If all birds have feathers, then all herons have feathers.

Proof: Assume that all birds have feathers. We will show that all herons have feathers.

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

$$\underbrace{(\forall b.\ (Bird(b) \to Feathers(b)))}_{\text{All birds have feathers}} \to \underbrace{(\forall h.\ (Heron(h) \to Feathers(h)))}_{\text{All herons have feathers}}$$

Proving vs. Assuming

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

$$(\forall b.\ (Bird(b) \to Feathers(b))) \to (\forall h.\ (Heron(h) \to Feathers(h)))$$

We never introduce a variable b.

We introduce a variable h 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.

$$(\forall b.\ (Bird(b) \to Feathers(b))) \to (\forall h.\ (Heron(h) \to Feathers(h)))$$

We never introduce a variable b.

We introduce a variable h 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, have feathers.

$$(\forall b.\ (Bird(b) \to Feathers(b))) \to (\forall h.\ (Heron(h) \to Feathers(h)))$$

We never introduce a variable b.

We introduce a variable h almost immediately.

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

$$(\forall x \in A.\ f(f(x)) = x) \quad \rightarrow \quad (\forall b \in A.\ \exists a \in A.\ f(a) = b)$$

Assume this.

Prove this.

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

$(\forall x \in A.\ f(f(x)) = x) \rightarrow (\forall b \in A.\ \exists a \in A.\ f(a) = b)$

Assume this.

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 $f : A \rightarrow A$, if f is an involution, then f is surjective.

$$(\forall x \in A.\ f(f(x)) = x) \rightarrow (\forall b \in A.\ \exists a \in A.\ f(a) = b)$$

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 $f : A \rightarrow A$, if f is an involution, then f is surjective.

$(\forall x \in A.\ f(f(x)) = x) \quad \to \quad (\forall b \in A.\ \exists a \in A.\ f(a) = b)$

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

Prove this.

What do you do to prove
$\forall b \in A.$ [something]?

Answer at
https://cs103.stanford.edu/pollev

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.

$$(\forall x \in A.\ f(f(x)) = x) \rightarrow (\forall b \in A.\ \exists a \in A.\ f(a) = b)$$

Assume this.

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 $f : A \rightarrow A$, if f is an involution, then f is surjective.

$(\forall x \in A.\ f(f(x)) = x) \rightarrow (\forall b \in A.\ \exists a \in A.\ f(a) = b)$

Ass

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

Prove this.

Proof Outline

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

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

$$(\forall x \in A.\ f(f(x)) = x) \rightarrow (\forall b \in A.\ \exists a \in A.\ f(a) = b)$$

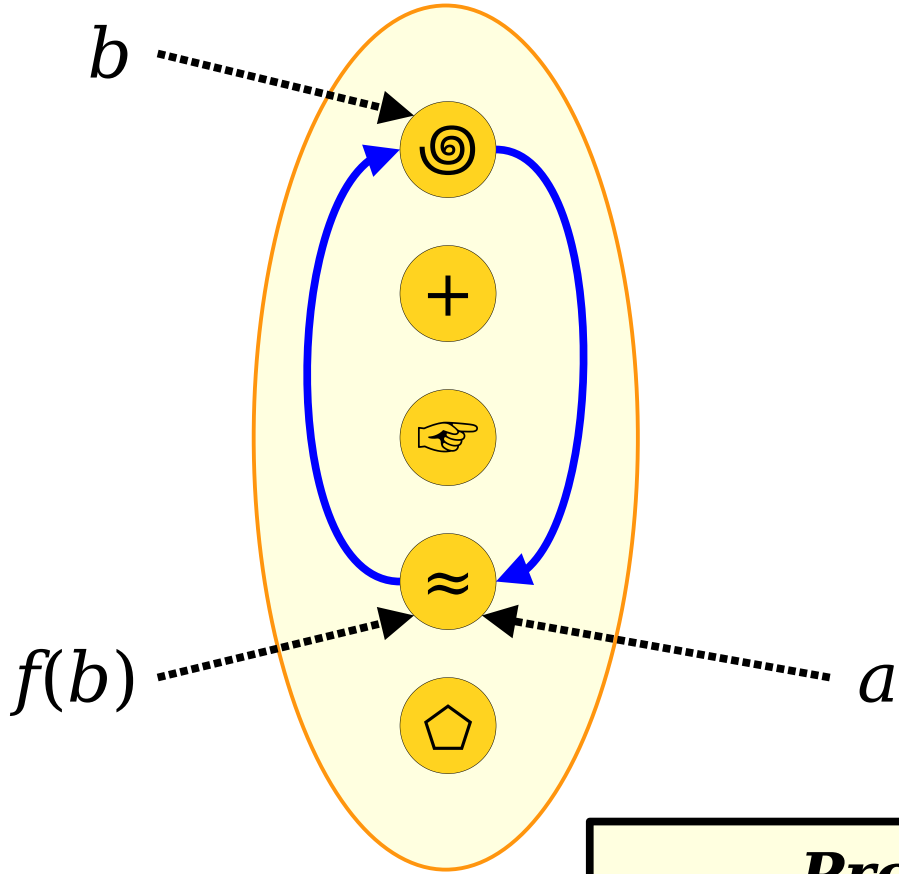
Now, we hit an existential quantifier. Since we're *proving* this, we need to find a choice of $a \in A$ where this is true.

Prove this.

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 $f : A \rightarrow A$, 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. ■

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

The Two-Column Proof Organizer

Theorem: Let $f : A \to A$ be an involution. Then f is injective.

Theorem: Let $f : A \to A$ be an involution. Then f is injective.

What We're Assuming	***What We Need to Prove***
$f : A \to A$ is an involution.	f is injective.
$\forall z \in A.\ f(f(z)) = z.$	$\forall a_1 \in A.\ \forall a_2 \in A.\ (f(a_1) = f(a_2) \to a_1 = a_2)$

We're *assuming* this universally-quantified statement, so we won't introduce a variable for what's here.

We need to *prove* this universally-quantified statement. So let's introduce arbitrarily-chosen values.

Theorem: Let $f : A \to A$ be an involution.
Then f is injective.

What We're Assuming	***What We Need to Prove***
$f : A \to A$ is an involution.	f is injective.
$\forall z \in A.\ f(f(z)) = z.$	~~$\forall a_1 \in A.\ \forall a_2 \in A.$~~ $(f(a_1) = f(a_2) \to a_1 = a_2)$
$a_1 \in A$	
$a_2 \in A$	

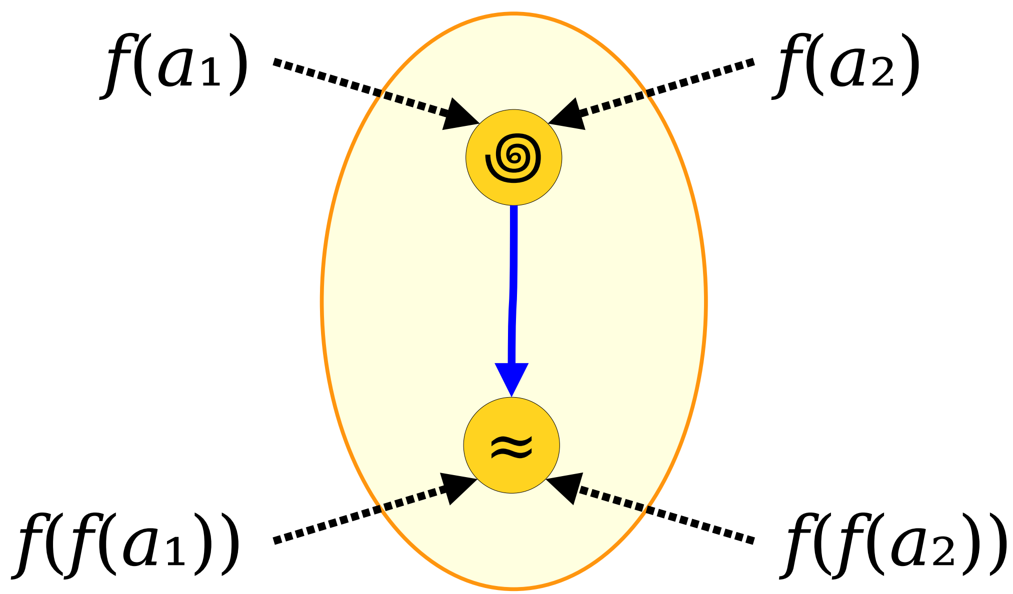
Theorem: Let $f : A \to A$ be an involution. Then f is injective.

What We're Assuming	What We Need to Prove
$f : A \to A$ is an involution.	f is injective.
$\forall z \in A.\ f(f(z)) = z.$	~~$\forall a_1 \in A.\ \forall a_2 \in A.$~~ $(f(a_1) = f(a_2) \to a_1 = a_2)$
$a_1 \in A$	
$a_2 \in A$	

We need to prove this implication. So we assume the antecedent and prove the consequent.

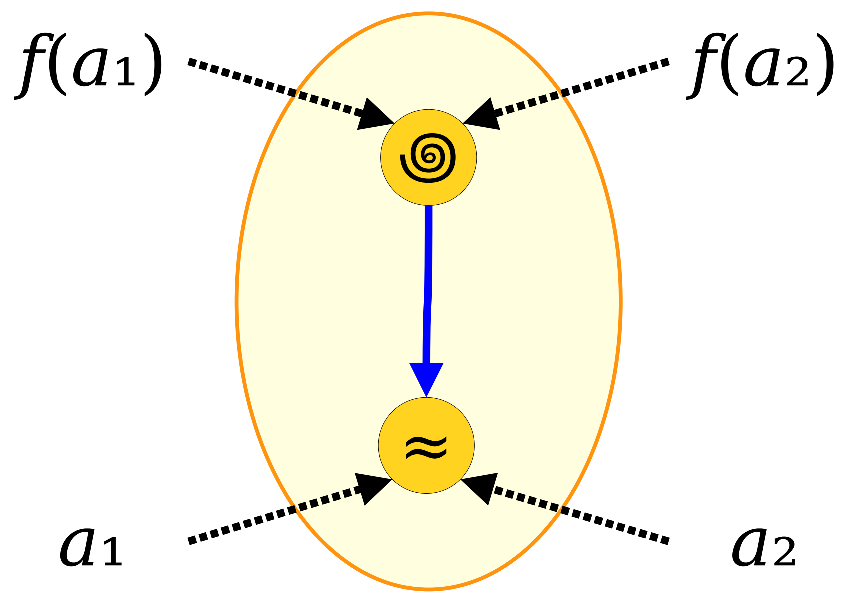
Theorem: Let $f : A \to A$ be an involution.
Then f is injective.

What We're Assuming	***What We Need to Prove***
$f : A \to A$ is an involution.	f is injective.
$\forall z \in A.\ f(f(z)) = z.$	~~$\forall a_1 \in A.\ \forall a_2 \in A.\ (f(a_1) = f(a_2) \to$~~ $a_1 = a_2$ ~~$)$~~
$a_1 \in A$	
$a_2 \in A$	
$f(a_1) = f(a_2)$	



Theorem: Let $f : A \to A$ be an involution. Then f is injective.

What We're Assuming	***What We Need to Prove***
$f : A \to A$ is an involution.	f is injective.
$\forall z \in A.\ f(f(z)) = z.$	~~$\forall a_1 \in A.\ \forall a_2 \in A.\ (f(a_1) = f(a_2) \to$~~ $a_1 = a_2$ ~~)~~
$a_1 \in A$	
$a_2 \in A$	
$f(a_1) = f(a_2)$	
$f(f(a_1)) = f(f(a_2))$	
$f(f(a_1)) = a_1$	
$f(f(a_2)) = a_2$	



Theorem: Let $f : A \to A$ be an involution. Then f is injective.

Proof: Choose any $a_1, a_2 \in A$ where $f(a_1) = f(a_2)$. We need to show that $a_1 = a_2$.

Since $f(a_1) = f(a_2)$, we know that $f(f(a_1)) = f(f(a_2))$. Because f is an involution, we see $a_1 = f(f(a_1))$ and that $f(f(a_2)) = a_2$. Putting this together, we see that

$$a_1 = f(f(a_1)) = f(f(a_2)) = a_2,$$

so $a_1 = a_2$, as needed. ■

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

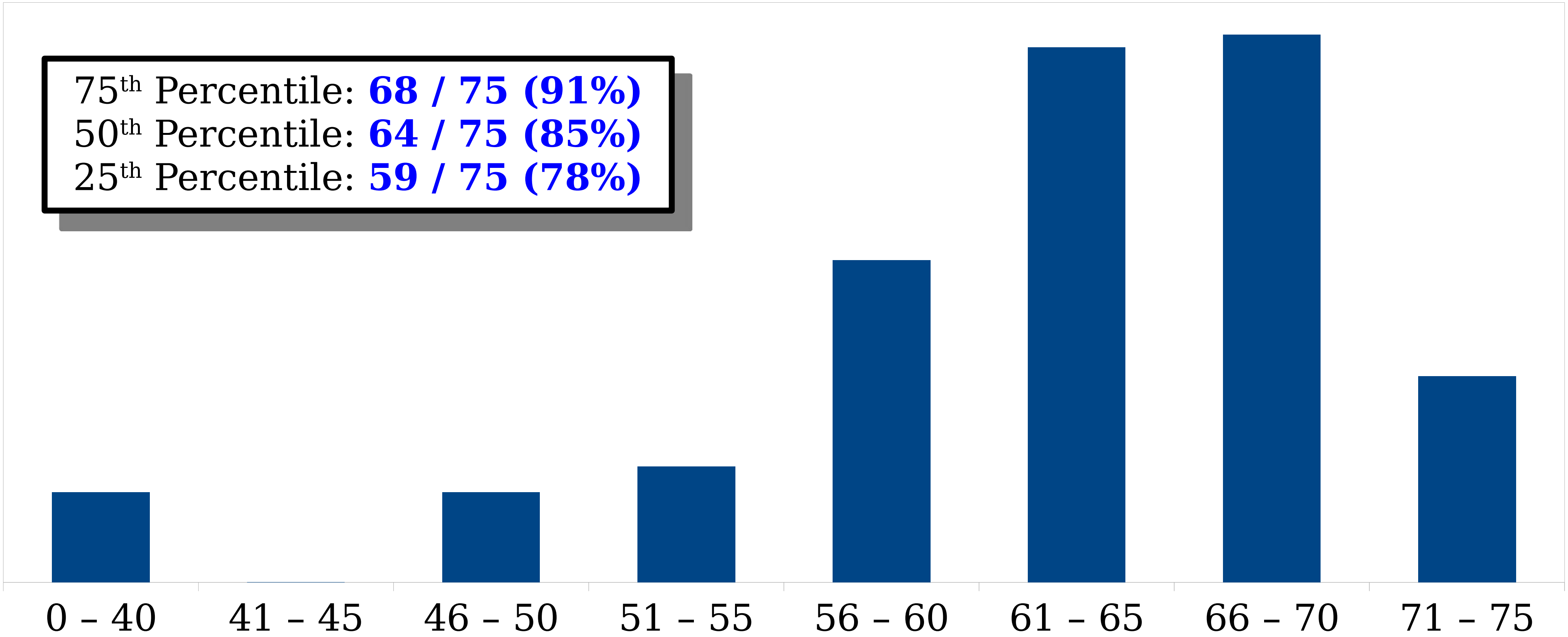
Time-Out for Announcements!

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

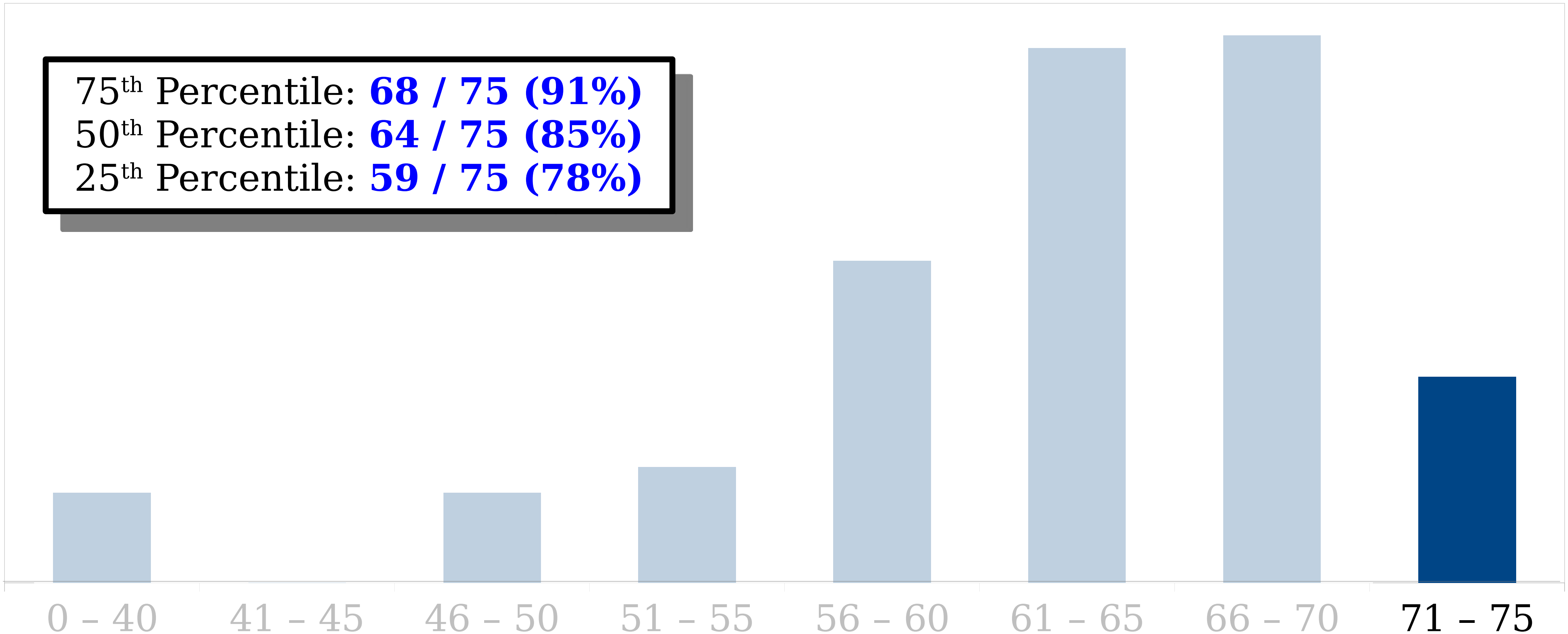
75th Percentile: **68 / 75 (91%)**
50th Percentile: **64 / 75 (85%)**
25th Percentile: **59 / 75 (78%)**



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.

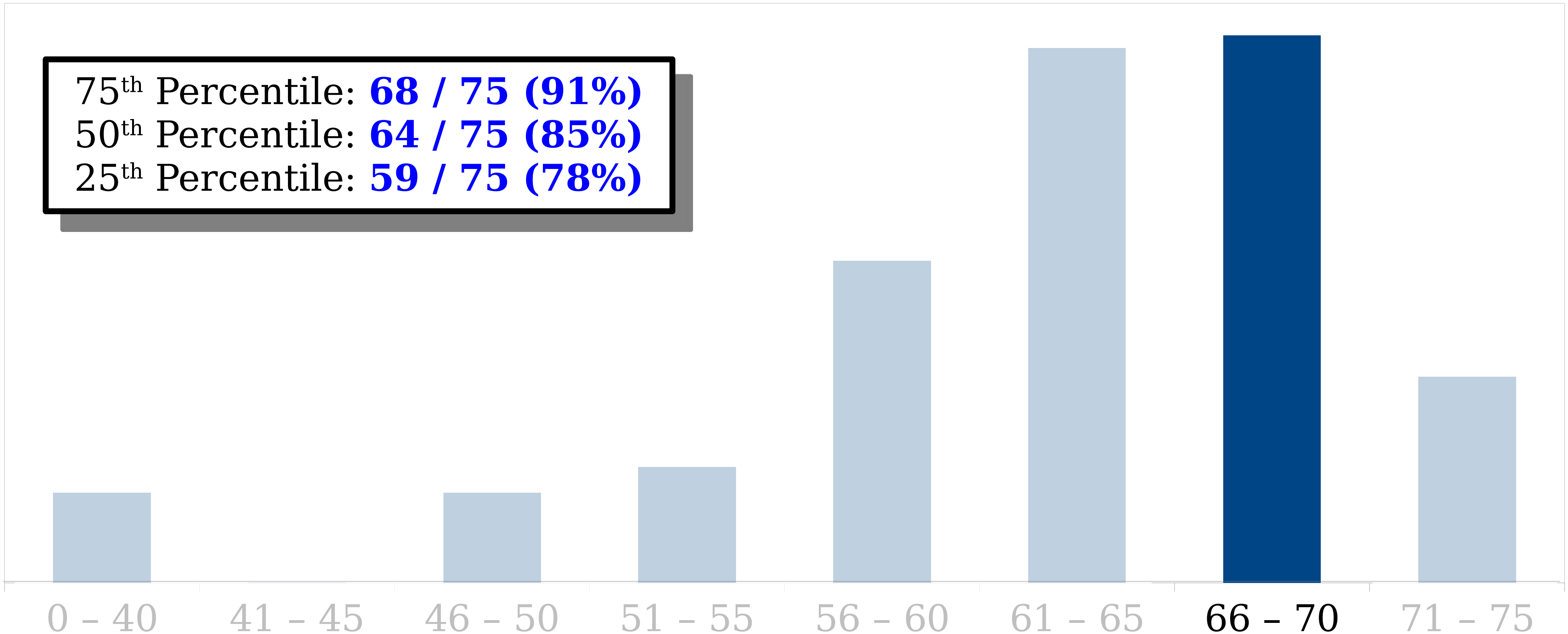
Problem Set One Graded



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

Problem Set One Graded

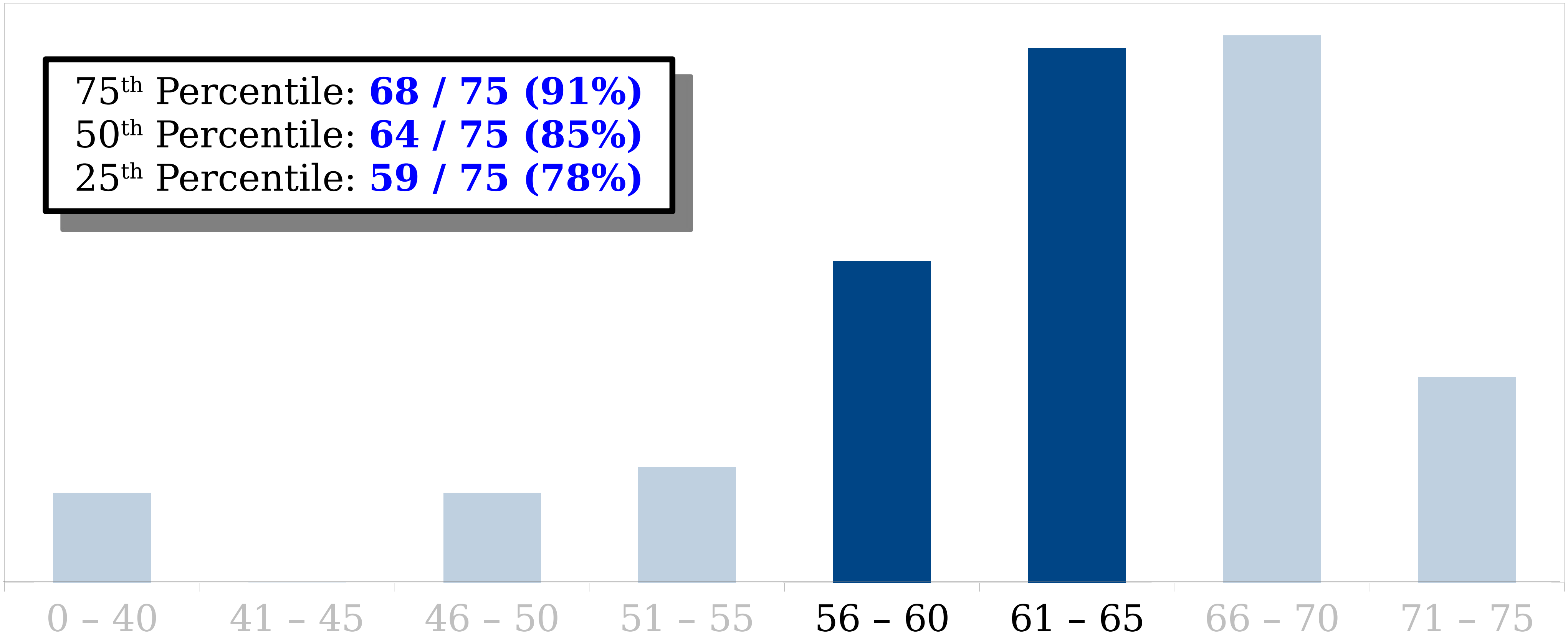
75th Percentile: **68 / 75 (91%)**
50th Percentile: **64 / 75 (85%)**
25th Percentile: **59 / 75 (78%)**



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

Problem Set One Graded

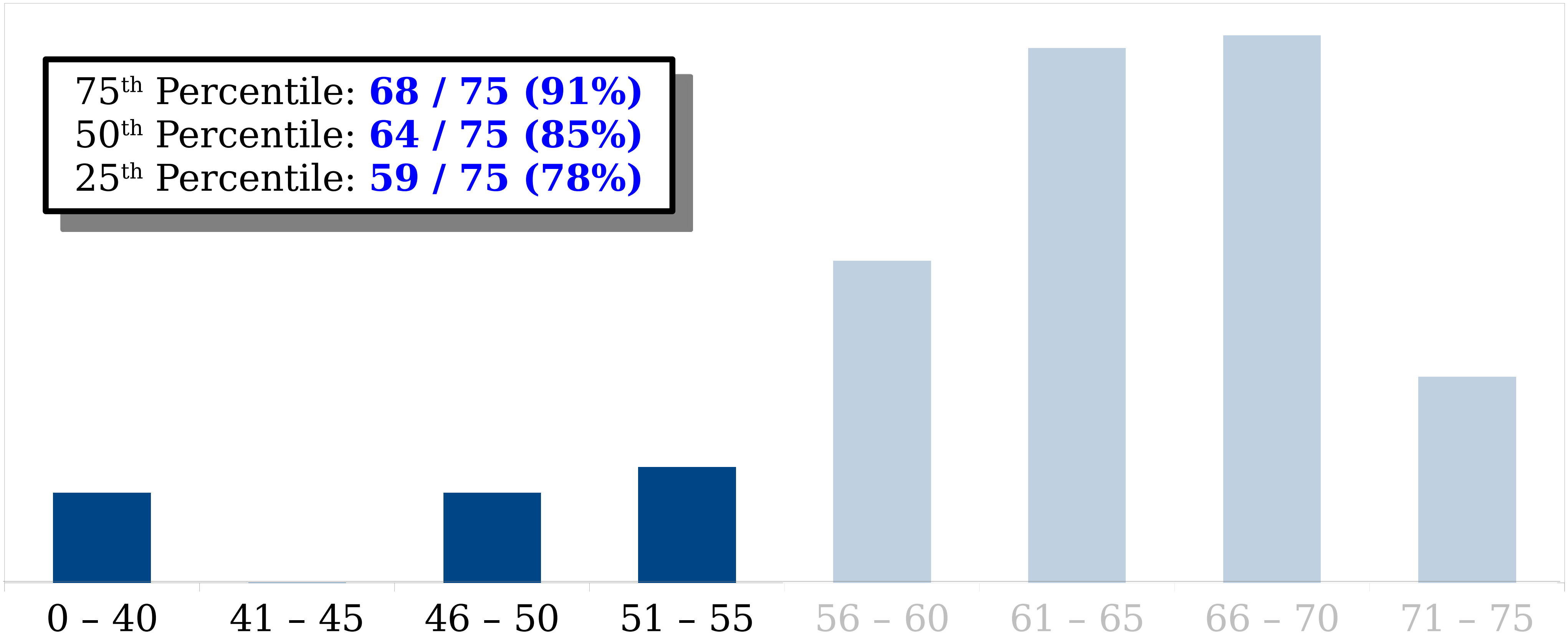
75th Percentile: **68 / 75 (91%)**
50th Percentile: **64 / 75 (85%)**
25th Percentile: **59 / 75 (78%)**



"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

75^{th} Percentile: **68 / 75 (91%)**
50^{th} Percentile: **64 / 75 (85%)**
25^{th} Percentile: **59 / 75 (78%)**



"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: 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

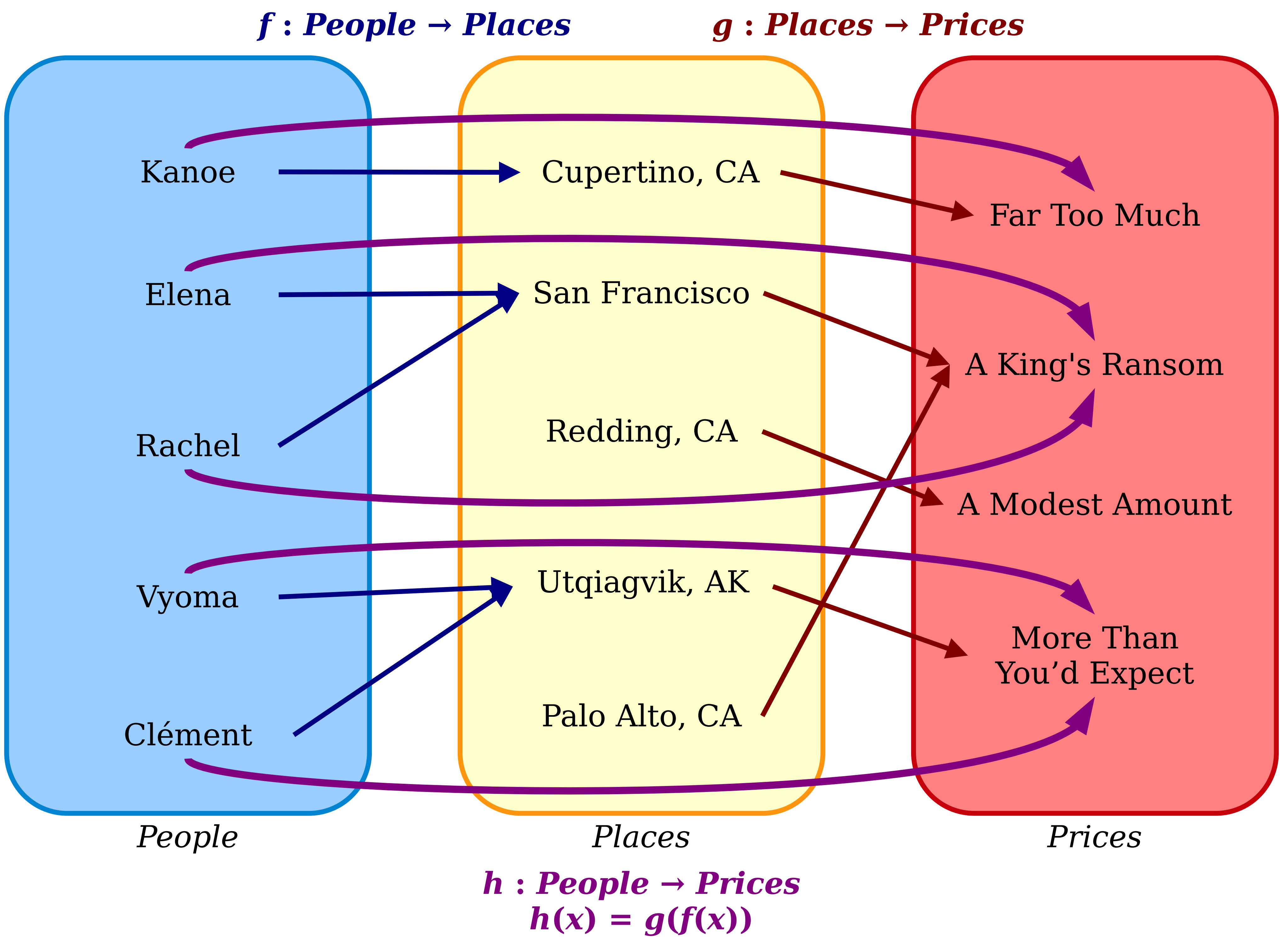
- We’re human. We make mistakes. And we’re happy to correct them!
- Regrades will open on Gradescope 48 hours after grades are released. They close one week after grades are released.
- Notes on regrades:
  - Please be civil. We make mistakes. We’re happy to correct them.
  - We have to grade what you 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.

Essential Action Items

- ***Review your feedback.***
  - Don’t just look at the raw score. Make sure you really, truly understand where you need to improve.
- ***Read the solutions in depth.***
  - Make sure you understand what we were asking, why we asked it, and what we wanted you to take away.
  - (Especially for Q8, Q10) Look at our solutions and see if there’s any neat lessons you can draw from them.
- ***Come to us with questions.***
  - Anything you’re not sure about? That’s what we’re here for! Come to office hours, ask questions on EdStem, etc.

Back to CS103!

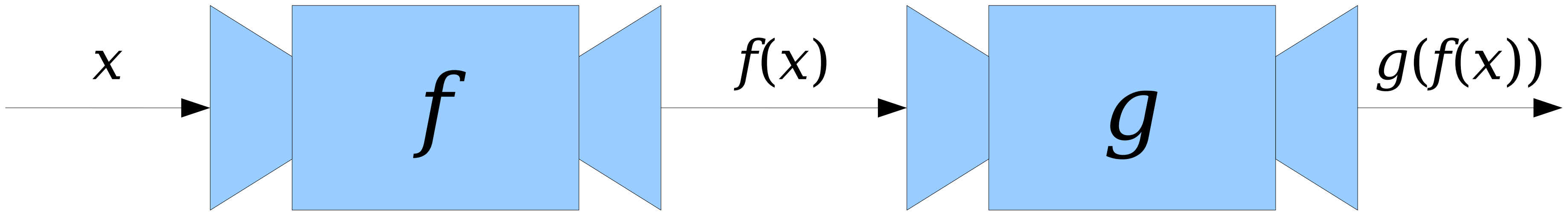
Function Composition



f : People → Places
g : Places → Prices
Kanoe
Elena
Rachel
Vyoma
Clément
Cupertino, CA
San Francisco
Redding, CA
Utqiagvik, AK
Palo Alto, CA
Far Too Much
A King's Ransom
A Modest Amount
More Than You'd Expect
People
Places
Prices
h : People → Prices
h(x) = g(f(x))

Function Composition

- Suppose that we have two functions $f : A \to B$ and $g : B \to C$.
- Notice that the codomain of f is the domain of g. This means that we can use outputs from f as inputs to g.



Function Composition

- Suppose that we have two functions $f : A \to B$ and $g : B \to C$.
- The ***composition of f and g***, denoted $\boldsymbol{g \circ f}$, is a function where
  - $g \circ f : A \to C$, and
  - $(g \circ f)(x) = g(f(x))$.
- A few things to notice:
  - The domain of $g \circ f$ is the domain of f. Its codomain is the codomain of g.
  - Even though the composition is written $g \circ f$, when evaluating $(g \circ f)(x)$, the function f is evaluated first.

The name of the function is $g \circ f$. When we apply it to an input x, we write $(g \circ f)(x)$. I don't know why, but that's what we do.

Properties of Composition

Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is an injection.

Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is an injection.

What We're Assuming

$f : A \to B$ is an injection.

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

$g : B \to C$ is an injection.

$$\forall x \in B.\ \forall y \in B.\ (x \neq y \to g(x) \neq g(y))$$

We're *assuming* these universally-quantified statements, so we won't introduce any variables for what's here.

What We Need to Prove

$g \circ f$ is an injection.

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

We need to *prove* this universally-quantified statement. So let's introduce arbitrarily-chosen values.

Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is an injection.

What We're Assuming	***What We Need to Prove***
$f : A \to B$ is an injection.	$g \circ f$ is an injection.
$\forall x \in A.\ \forall y \in A.\ (x \neq y \to$ $f(x) \neq f(y)$ $)$	$\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to$ $(g \circ f)(a_1) \neq (g \circ f)(a_2)$ $)$
$g : B \to C$ is an injection.	We need to *prove* this universally-quantified statement. So let's introduce arbitrarily-chosen values.
$\forall x \in B.\ \forall y \in B.\ (x \neq y \to$ $g(x) \neq g(y)$ $)$	
$a_1 \in A$ is arbitrarily-chosen.	
$a_2 \in A$ is arbitrarily-chosen.	

Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is an injection.

What We're Assuming

$f : A \to B$ is an injection.

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

$g : B \to C$ is an injection.

$\forall x \in B.\ \forall y \in B.\ (x \neq y \to$
$g(x) \neq g(y)$
$)$

$a_1 \in A$ is arbitrarily-chosen.

$a_2 \in A$ is arbitrarily-chosen.

$a_1 \neq a_2$

What We Need to Prove

$g \circ f$ is an injection.

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

Now we're looking at an implication. Let's *assume* the antecedent and *prove* the consequent.

Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is an injection.

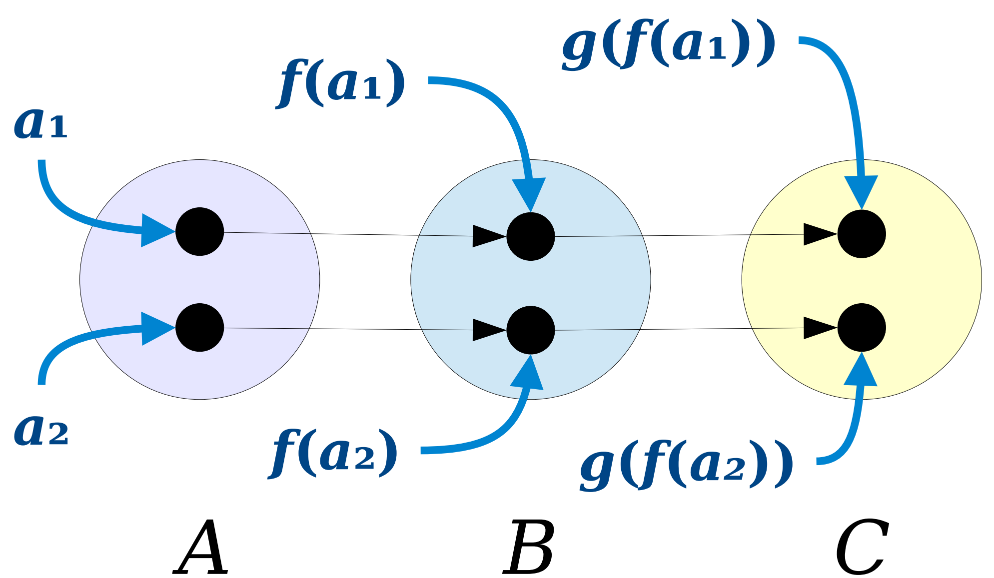
What We're Assuming	***What We Need to Prove***
$f : A \to B$ is an injection.	$g \circ f$ is an injection.
$\forall x \in A. \forall y \in A. (x \neq y \to f(x) \neq f(y))$	$\forall a_1 \in A. \forall a_2 \in A. (a_1 \neq a_2 \to (g \circ f)(a_1) \neq (g \circ f)(a_2))$
$g : B \to C$ is an injection.	Let's write this out separately and simplify things a bit.
$\forall x \in B. \forall y \in B. (x \neq y \to g(x) \neq g(y))$	
$a_1 \in A$ is arbitrarily-chosen.	
$a_2 \in A$ is arbitrarily-chosen.	
$a_1 \neq a_2$	

Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is an injection.

What We're Assuming	***What We Need to Prove***
$f : A \to B$ is an injection.	$g \circ f$ is an injection.
$\forall x \in A.\ \forall y \in A.\ (x \neq y \to f(x) \neq f(y))$	$\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to (g \circ f)(a_1) \neq (g \circ f)(a_2))$
$g : B \to C$ is an injection.	$g(f(a_1)) \neq g(f(a_2))$
$\forall x \in B.\ \forall y \in B.\ (x \neq y \to g(x) \neq g(y))$	
$a_1 \in A$ is arbitrarily-chosen.	
$a_2 \in A$ is arbitrarily-chosen.	
$a_1 \neq a_2$	

Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is an injection.

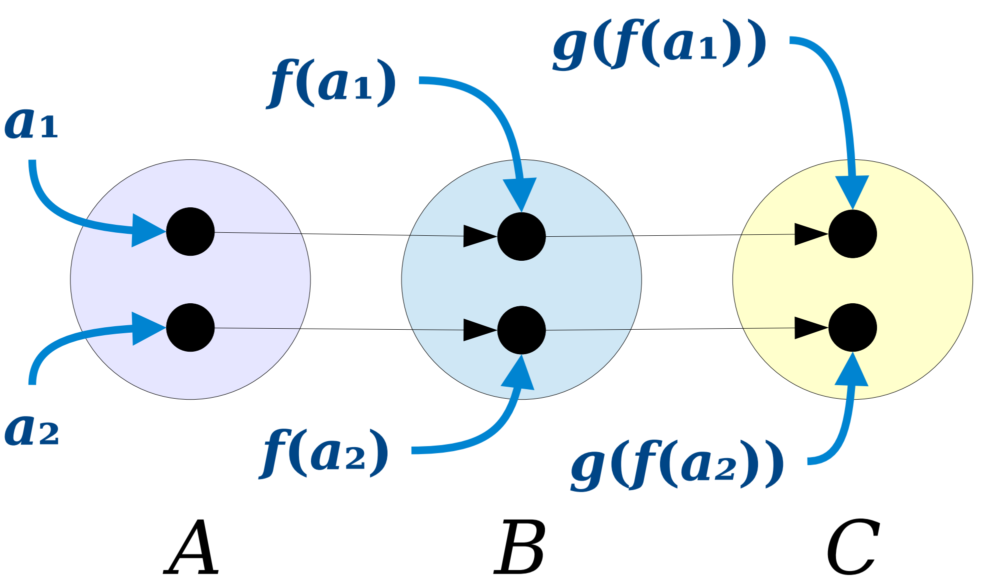
What We're Assuming	***What We Need to Prove***
$f : A \to B$ is an injection.	$g \circ f$ is an injection.
$\forall x \in A.\ \forall y \in A.\ (x \neq y \to f(x) \neq f(y))$	$\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to (g \circ f)(a_1) \neq (g \circ f)(a_2))$
$g : B \to C$ is an injection.	$g(f(a_1)) \neq g(f(a_2))$
$\forall x \in B.\ \forall y \in B.\ (x \neq y \to g(x) \neq g(y))$	
$a_1 \in A$ is arbitrarily-chosen.	
$a_2 \in A$ is arbitrarily-chosen.	
$a_1 \neq a_2$	



Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is also an injection.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary injections. We will prove that the function $g \circ f : A \to C$ is also injective. To do so, consider any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We will prove that $(g \circ f)(a_1) \neq (g \circ f)(a_2)$. Equivalently, we need to show that $g(f(a_1)) \neq g(f(a_2))$.

Since f is injective and $a_1 \neq a_2$, we see that $f(a_1) \neq f(a_2)$. Then, since g is injective and $f(a_1) \neq f(a_2)$, we see that $g(f(a_1)) \neq g(f(a_2))$, as required. ■

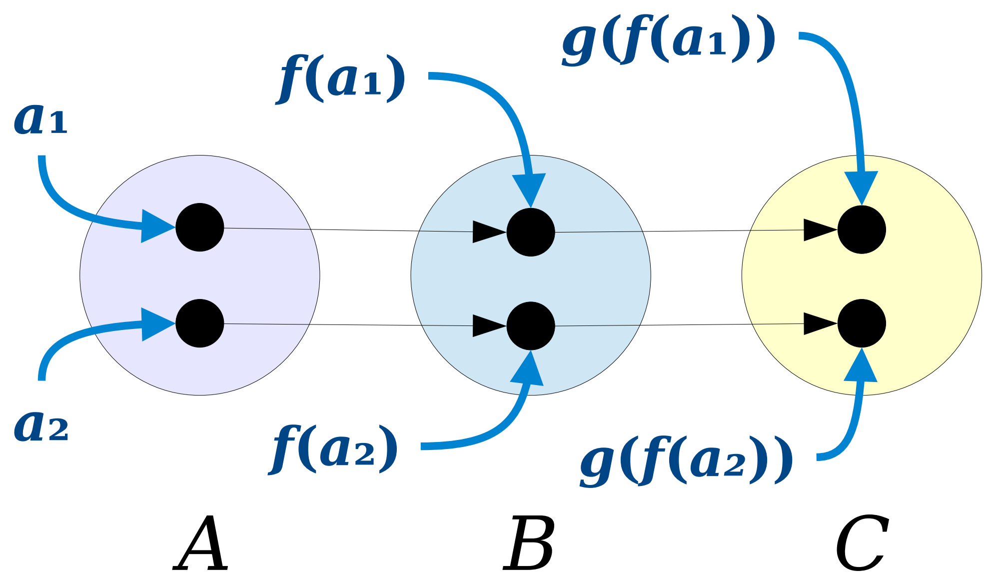


Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is also an injection.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary injections. We will prove that the function $g \circ f : A \to C$ is also injective. To do so, consider any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We will prove that $(g \circ f)(a_1) \neq (g \circ f)(a_2)$. Equivalently, we need to show that $g(f(a_1)) \neq g(f(a_2))$.

Since f is injective and $a_1 \neq a_2$, we see that $f(a_1) \neq f(a_2)$. Then, since g is injective and $f(a_1) \neq f(a_2)$, we see that $g(f(a_1)) \neq g(f(a_2))$, as required. ■

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



Theorem: If $f : A \to B$ is a surjection and $g : B \to C$ is a surjection, then the function $g \circ f : A \to C$ is a surjection.

Proof: In the appendix!

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.

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

- ***Set Theory Revisited***
  - Formalizing our definitions.
- ***Proofs on Sets***
  - How to rigorously establish set-theoretic results.

Appendix: Additional Function Proofs

Proof: Composing surjections yields a surjection.

Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary surjections. We will prove that the function $g \circ f : A \to C$ is also surjective. To do so, we will prove that for any $c \in C$, there is some $a \in A$ such that $(g \circ f)(a) = c$. Equivalently, we will prove that for any $c \in C$, there is some $a \in A$ such that $g(f(a)) = c$.

Consider any $c \in C$. Since $g : B \to C$ is surjective, there is some $b \in B$ such that $g(b) = c$. Similarly, since $f : A \to B$ is surjective, there is some $a \in A$ such that $f(a) = b$. Then we see that

$$g(f(a)) = g(b) = c,$$

which is what we needed to show. ■