

1. Proving Injectivity and Surjectivity

- a. What does the notation $f : A \rightarrow B$ mean? Which sets are the domain and codomain? Explain what the domain and codomain are.

This notation says that f is a function with domain A and codomain B . In other words, f 's inputs are objects from the set A and its outputs are objects from the set B .

- b. Here are two ways to state the definition of injectivity:

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

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

- (1) Explain what an injective function is in your own words.

Some explanations are:

- Unequal inputs produce unequal outputs
- If we have two equal outputs, they must have come from the same input
- Each element of the codomain has at most one element of the domain that maps to it
- Given an element from the codomain, it's impossible to come up with two different elements of the domain that map to it

- (2) What's the difference between this definition of an injective function and the following property, which is one of the requirements for something to be called a function?

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

This property says that equal **inputs** produce equal **outputs**. The definition of injectivity means that equal **outputs** produce equal **inputs** (or, equivalently, unequal inputs produce unequal outputs.)

- (3) Based on the structure of each formula, what are two ways to prove that f is injective?

For the first definition, we'd consider arbitrary $a_1, a_2 \in A$ where $a_1 \neq a_2$. We'd then show that $f(a_1) \neq f(a_2)$.

For the second definition, we'd consider arbitrary $a_1, a_2 \in A$ where $f(a_1) = f(a_2)$. We'd then show that $a_1 = a_2$.

- (4) Negate either formula and simplify it. How would you prove that f is **not** injective?

This is the negation of the formula:

$$\exists a_1 \in A. \exists a_2 \in A. (a_1 \neq a_2 \wedge f(a_1) = f(a_2))$$

To prove that f is not injective, we would need to find non-equal $a_1, a_2 \in A$ where $f(a_1) = f(a_2)$. In other words, finding different inputs that produce the same output means that a function is not injective.

c. Here's the definition of surjectivity:

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

(1) Explain what a surjective function is in your own words.

Some explanations are:

- Given an element from the codomain, there has to be something from the domain that maps to it
- Each element of the codomain has at least one element of the domain that maps to it
- The entire codomain is “covered” by the results of the function

(2) What's the difference between this definition of a surjective function and the following property, which is one of the requirements for something to be called a function?

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

This property says that for every **domain element**, a codomain element is produced when the function is applied: all the inputs will produce valid outputs.

The definition of surjectivity says that for every **codomain element**, there is at least one domain element that produces it when the function is applied: all the outputs have some input that produces them.

(3) Based on the structure of this formula, how would you write a proof that f is surjective?

Consider an arbitrary element $b \in B$. Then, demonstrate how to find an a in A where $f(a) = b$.

(4) Negate the formula and simplify it. How would you write a proof that f is **not** surjective?

The negation of the formula is:

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

To prove that f is not surjective, we would need to find an output b that cannot possibly be produced by any input to the function.

One way to write this formula to more clearly correspond to this English-language intuition would be $\exists b \in B. \neg(\exists a \in A. f(a) = b)$

- d. How would you write a proof that a function f is (1) bijective, (2) **not** bijective?

To prove that f is bijective, prove it's injective and prove it's surjective.

To prove that f is not bijective, either prove it's not injective or prove it's not surjective.

2. Function Composition

For these questions, use the following strategies: (1) Write out all of the definitions in the problem. (2) Use the proof strategies table to determine what you will **assume** and **want to show**. (3) Use the two-column proof organizer to keep track of introducing new variables, expanding definitions, and so on.

- a. Let $f : A \rightarrow B$ and $g : B \rightarrow C$ be functions. Prove that if $g \circ f$ is injective, then f is injective.

Proof: Let $f : A \rightarrow B$ and $g : B \rightarrow C$ be functions where $g \circ f : A \rightarrow C$ is injective. We'll show that f is injective. Consider two elements $a_1, a_2 \in A$ where $a_1 \neq a_2$; we'll show that $f(a_1) \neq f(a_2)$. Because $g \circ f$ is injective, we know that $(g \circ f)(a_1) \neq (g \circ f)(a_2)$, or equivalently that $g(f(a_1)) \neq g(f(a_2))$. Because g is a function, we see that $f(a_1) \neq f(a_2)$, as required. ■

- b. Let $f : A \rightarrow B$ and $g : B \rightarrow C$ be functions. Prove that if $g \circ f$ is surjective, then g is surjective.

Proof: Let $f : A \rightarrow B$ and $g : B \rightarrow C$ be functions where $g \circ f : A \rightarrow C$ is surjective. We'll show that g is surjective. Pick an arbitrary $c \in C$. Since $g \circ f$ is surjective, there exists some $a \in A$ where $(g \circ f)(a) = c$, or equivalently $g(f(a)) = c$. Then, we can see that there is an element b in B , namely $f(a)$, where $g(b) = c$, as required. ■

3. First-Order Definitions and Functions Proofs

Interpreting definitions given in terms of first-order logic is really important for the remainder of CS 103. In this problem, we'll practice with setting up proofs involving first-order logic.

- a. Let $f : A \rightarrow B$ be a function. We call f **right-cancellative** if the following property holds for any functions $g : B \rightarrow C$ and $h : B \rightarrow C$:

$$(\forall a \in A.(g \circ f)(a) = (h \circ f)(a)) \rightarrow (\forall b \in B.g(b) = h(b))$$

Prove that if f is surjective, then f is right-cancellative.

Key question: When we want to show an implication, what should we do?

One way to set up this proof: We should assume the antecedent and prove the consequent. In this problem, this means we assume f is surjective and show f is right-cancellative. The definition of right-cancellative is another implication, so again, we should assume the antecedent and show the consequent. Since we want to show a universally quantified statement, we pick an arbitrary $b \in B$ and we need to show that $g(b) = h(b)$.

Proof: Let $f : A \rightarrow B$ be a surjective function. We'll show that f is right-cancellative. To do so, let $g : B \rightarrow C$ and $h : B \rightarrow C$ be functions where for all $a \in A$, we have that $(g \circ f)(a) = (h \circ f)(a)$, and pick an element $b \in B$. We'll show that $g(b) = h(b)$.

Because f is surjective and $b \in B$, we know that there must be an element $a \in A$ where $f(a) = b$. Then, that means we can write $g(b) = (g \circ f)(a) = (g \circ f)(a)$. Similarly, we can write $h(b) = (h \circ f)(a) = (h \circ f)(a)$. Then, because $a \in A$, based on our assumption, we can see that $(g \circ f)(a) = (h \circ f)(a)$, meaning that $g(b) = h(b)$, and so f is right-cancellative, as required. ■

4. Set Theory Proofs

If we have time, we'll prove the following result as a group: for arbitrary sets A and B , $\wp(A) \cap \wp(B) \subseteq \wp(A \cap B)$.

Proof: Pick some $S \in \wp(A) \cap \wp(B)$. We need to show that $S \in \wp(A \cap B)$, equivalently that S is a subset of $A \cap B$. To do this, pick an arbitrary element $x \in S$, and we will show that x is in $A \cap B$.

Since S is an element in $\wp(A) \cap \wp(B)$, we know that S is also an element in $\wp(A)$, or in other words, $S \subseteq A$. This means that x is an element in A . Similarly, we can see that S is an element in $\wp(B)$, or in other words, $S \subseteq B$, meaning that x is also an element in B . Since x is in both A and B , we can see that $x \in A \cap B$ as required. ■

For the following proofs, proceed by clearly articulating what you are assuming and what you want to show, unpacking definitions, and focusing on individual elements of sets. In these statements, A , B , and C are arbitrary sets.

- a. Prove that if $A \subseteq B$, then $A \cap C \subseteq B \cap C$.

Proof: Let A , B , and C be arbitrary sets where $A \subseteq B$. We will show that $A \cap C \subseteq B \cap C$. Pick some $x \in A \cap C$. We need to show that $x \in B \cap C$, or equivalently, that $x \in B$ and $x \in C$. First, since x is in $A \cap C$, we know that x is in A . Then, since we know that $A \subseteq B$, we also know that $x \in B$. Second, since x is in $A \cap C$, then x is also in C . Therefore, we've shown that $x \in B \cap C$, so we see that $A \cap C \subseteq B \cap C$, which is what we wanted to show. ■

- b. Prove that $\wp(A \cap B) \subseteq \wp(A) \cap \wp(B)$.

In conjunction with the result we proved, this means that $\wp(A \cap B) = \wp(A) \cap \wp(B)$. Nifty!

Proof: Pick any $S \in \wp(A \cap B)$. We want to show that $S \in \wp(A) \cap \wp(B)$, meaning that we want to show that $S \in \wp(A)$ and $S \in \wp(B)$. Equivalently, we want to show that $S \subseteq A$ and $S \subseteq B$.

To do this, consider any $x \in S$. Since we know $S \in \wp(A \cap B)$, or in other words $S \subseteq A \cap B$, we see that $x \in A \cap B$ as well. This means that $x \in A$ and $x \in B$, so we see that $S \subseteq A$ and $S \subseteq B$, as required. ■