1. Proofs with Functions and First-Order Properties

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

$$\big(\forall a \in A.\ (f \circ g)(a) = (f \circ h)(a)\big) \to \big(\forall a \in A.\ g(a) = h(a)\big)$$

Prove that if f is injective, then f is left-cancellative.

Proof: Let $f : B \to C$ be an injective function. We'll show that f is left-cancellative. To do this, take any functions $g : A \to B$ and $h : A \to B$ where, for all $a \in A$, we have that $(f \circ g)(a) = (f \circ h)(a)$. Pick an arbitrary $a \in A$, and we will show that $g(a) = h(a)$. Equivalently, thanks to f being injective, we will show that $f(g(a)) = f(h(a))$. To do so, consider that $f(g(a)) = (f \circ g)(a)$ and $f(h(a)) = (f \circ h)(a)$. By our assumption about $(f \circ g)$ and $(f \circ h)$, this means that $f(g(a)) = f(h(a))$ as required, and f is left-cancellative. ■

b. Let's say a function $f : A \to A$ is called **idempotent** if the following property holds:

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

Prove that if f is idempotent, either f is defined as $f(x) = x$ or f is not injective.

Key questions: To show an "or" statement, what should we do? How do we show that a function is not injective? What is a first-order logic statement with the meaning "f is defined as $f(x) = x$"?

One way to set up this proof: Overall, this theorem is an implication, so we should assume the antecedent and prove the consequent. In this problem, this means we assume f is idempotent and show either f is defined as $f(x) = x$ or f is not injective. This want-to-show statement involves "or", so we can set it up by showing that if f is not defined as $f(x) = x$, then f is not injective. Again, this is an implication, so we'll assume f is not defined as $f(x) = x$, and prove that f is not injective. (Note: We could also show this implication by contrapositive, but I'll proceed with a direct proof to demonstrate a proof of non-injectivity.) First, $f(x) = x$ means that $f(x) = x$ for all $x \in A$, so assuming that f is NOT defined as $f(x) = x$ means that we assume there exists an $x \in A$ where $f(x) \neq x$. Finally, to show that f is not injective, we need to find two values in f's domain that map to the same value in f's codomain.

Proof: Let $f : A \to B$ be an idempotent function. We'll show that either f is defined as $f(x) = x$ or f is not injective; to do so, assume that f is not defined as $f(x) = x$ and we'll show that f is not injective. To do so, we'll show that for some elements $x_1 \in A$ and $x_2 \in A$, $x_1 \neq x_2$ and $f(x_1) = f(x_2)$.

Because f is not defined as $f(x) = x$, we know that there is some $a \in A$ where $f(a) \neq a$. Consider $x_1 = a$ and $x_2 = f(a)$, meaning that $x_1 \neq x_2$. We can see that $f(x_1) = f(a)$ and $f(x_2) = f(f(a))$, and because f is an idempotent function, we see that $f(f(a)) = f(a)$, meaning $f(x_1) = f(x_2)$. Overall, this choice of x_1 and x_2 demonstrates that f is not injective, as required. ■

2. Injectivity and Surjectivity (challenge problem)

For these problems, we need some notation that won't come up elsewhere in CS 103. Let $\mathbb{Z}^2$ be the set $\{(m, n) \mid m \in \mathbb{Z} \land n \in \mathbb{Z}\}$. In plain English, this is the set of "ordered pairs" of integers. Some examples of elements in this set are $(103, 106)$ and $(-137, 0)$. Unlike sets, repeats are allowed, so $(-1, -1)$ is a perfectly valid element of $\mathbb{Z}^2$. Also unlike sets, the order matters, so $(103, 106)$ is different from $(106, 103)$.

When two ordered pairs (x_1, y_1) and (x_2, y_2) are equal, we know both that $x_1 = x_2$ and that $y_1 = y_2$.

c. Let $h : \mathbb{Z} \to \mathbb{Z}$ be an injective function. Define a function $f : \mathbb{Z}^2 \to \mathbb{Z}^2$ as follows:

$$f(x, y) = (h(x), h(x) + h(y))$$

First, to ensure you understand this definition, consider the case where h is defined as $h(n) = 2n$. Then, evaluate the following:

- $f(1, 1)$

  $f(1, 1) = (h(1), h(1) + h(1)) = (2, 4)$

- $f(0, -3)$

  $f(0, -3) = (h(0), h(0) + h(-3)) = (0, -6)$

Then, prove that f is injective. (Write your proof in general, not for our specific choice of $h(n)$ above.)

Hints:

- The elements of the domain and codomain of f are both elements of $\mathbb{Z}^2$, so they are both ordered pairs.
- There are two ways to structure a proof of injectivity. In this case, one of them leads to a much easier proof. If you're not finding the problem approachable, try switching your approach!
- You'll need to use the fact that h is injective twice.

Proof: Pick two arbitrary elements of $\mathbb{Z}^2$, (x, y) and (a, b), where $f(x, y) = f(a, b)$. We will show that $(x, y) = (a, b)$.

Since we know that $(h(x), h(x) + h(y)) = (h(a), h(a) + h(b))$, we can see that

$$h(x) = h(a)$$

and

$$h(x) + h(y) = h(a) + h(b).$$

Substituting $h(a)$ for $h(x)$ in the second equation, we see that $h(y) = h(b)$.

Because h is injective and $h(x) = h(a)$, we know that $x = a$. And because h is injective and $h(y) = h(b)$, we know that $y = b$. We can conclude that $(x, y) = (a, b)$, and f is injective, which is what we needed to show. ■

d. Let $h : \mathbb{Z} \to \mathbb{Z}$ be a surjective function. Define a function $f : \mathbb{Z}^2 \to \mathbb{Z}$ as follows:

$$f(x, y) = h(x) + h(y)$$

Prove that f is surjective.

Proof: Pick any $b \in \mathbb{Z}$.

Since h is surjective and 0 and b are integers, we know that there is an integer x_1 where $h(x_1) = 0$ and there is an integer x_2 where $h(x_2) = b$.

Now, consider $a = (x_1, x_2)$. We will show that $f(a) = b$. To see this, notice that

$$\begin{aligned} f(a) &= f(x_1, x_2) \\ &= h(x_1) + h(x_2) \\ &= 0 + b \\ &= b. \end{aligned}$$

Therefore, f is surjective. ■

These problems come from Professor Margaret Fleck at the University of Illinois's CS 173 class.

3. Set Union/Intersection Proofs

Let A, B, and C be arbitrary sets.

a. Prove that set union is distributive: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Proof: Let A, B, and C be sets. We'll show that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

First, we'll show that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. Consider any element $x \in A \cup (B \cap C)$. We'll show that x is in $(A \cup B) \cap (A \cup C)$. We have two cases: we know that x is either in A or in $B \cap C$. If x is in A, then it is in both $(A \cup B)$ and in $(A \cup C)$. If x is in $B \cap C$, then x is in both B and C, so x is also in $A \cup B$ and $A \cup C$. In either case, we've shown that x is in $(A \cup B) \cap (A \cup C)$.

Next, we'll show that $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. Consider any element x in $(A \cup B) \cap (A \cup C)$. We'll show that x is in $A \cup (B \cap C)$. We know that x is in both $A \cup B$ and $A \cup C$, so we have two cases: either x is in A or x is in B, and either x is in A or x is in C. Then, either x is in A, or x must be in both B and in C, so it is in $A \cup (B \cap C)$.

We've shown that $A \cup (B \cap C)$ and $(A \cup B) \cap (A \cup C)$ are subsets of each other, as required. ■

b. Prove that set intersection is distributive: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Proof: Let A, B, and C be sets. We'll show that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

First, we'll show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Consider any element $x \in A \cap (B \cup C)$. We'll show that x is in $(A \cap B) \cup (A \cap C)$. We know that x is in A and that x is in $B \cup C$, i.e. is either in B or in C, so we have two cases. If x is in B, then x is in $A \cap B$. If x is in C, then x is in $A \cap C$. In either case, we can see that $x \in (A \cap B) \cup (A \cap C)$.

Next, we'll show that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Consider any element x in $(A \cap B) \cup (A \cap C)$. We'll show that x is in $A \cap (B \cup C)$. We know that x is in either $A \cap B$ or $A \cap C$, so we have multiple cases. If x is in $A \cap B$, then we know that x is in A and x is in B, meaning that x is also in $B \cup C$. If x is in $A \cap C$, then we know that x is in a and x is in C, meaning that x is also in $B \cup C$. Either way, we can see that $x \in A \cap (B \cup C)$.

We've shown that $(A \cap B) \cup (A \cap C)$ and $A \cap (B \cup C)$ are subsets of each other, as required. ■

4. Set-Builder Notation and Power Set Proofs

Formally, for sets S and T, $S - T = \{x | x \in S \land x \notin T\}$. We can use this definition of set difference to practice writing proofs that use set-builder notation.

a. Prove that $A - B \subseteq A$.

> **Proof:** We'll show that $A - B \subseteq A$. To do so, pick an arbitrary element $x \in A - B$. We'll show that $x \in A$. By the definition of set subtraction, we know that $x \in A$ and $x \notin B$, so x is in A, which is what we wanted to show. ■

b. Prove that if $\wp(A) \subseteq C$, then $\wp(A - B) \subseteq C$. Feel free to use the previous part and the fact that, for any sets R, S, and T, if $S \subseteq T$ and $T \subseteq R$, then $S \subseteq R$.

> **Proof:** Assume that $\wp(A) \subseteq C$. We'll show that $\wp(A - B) \subseteq C$. To do so, pick an arbitrary element $S \in \wp(A - B)$. We'll show that it is also in C.
>
> Since $S \in \wp(A - B)$, we know that $S \subseteq A - B$. Because we know that $A - B \subseteq A$ as proved in the previous part, this also means that $S \subseteq A$. By the definition of power set, then, we know that $S \in \wp(A)$. And since we assumed $\wp(A) \subseteq C$, that means that $S \in C$, which is what we wanted to show. ■

c. Prove that $A \cap B = A - (A - B)$.

> **Proof:** We'll show that $A \cap B = A - (A - B)$. We'll do this by showing that $A \cap B \subseteq A - (A - B)$ and that $A - (A - B) \subseteq A \cap B$.
>
> First, we'll show that $A \cap B \subseteq A - (A - B)$. Pick an arbitrary element $x \in A \cap B$. We'll show that x is also in $A - (A - B)$ by showing that $x \in A$ and $x \notin A - B$. Since x is in $A \cap B$, we know that x is in A, and we also know that x is in B, meaning that it's not in $A - B$. Then, we've shown that $A \cap B \subseteq A - (A - B)$.
>
> Next, we'll show that $A - (A - B) \subseteq A \cap B$. Pick an arbitrary element $x \in A - (A - B)$. We'll show that x is also in $A \cap B$ by showing that $x \in A$ and $x \in B$. Because x is in $A - (A - B)$, we know that x is in A. We also know that x is not in $A - B$, meaning that it either is in B or is not in A; however, since we have previously seen that x is in A, we see that x must be in B. Then, we've shown that x is in both A and B, so we see that $x \in A \cap B$ and $A \cap B \subseteq A - (A - B)$.
>
> We conclude that $A \cap B = A - (A - B)$ as required. ■