PSET1

Student: Ryan Baldwin, `rbaldwi2@swarthmore.edu`
Lecturer: Dr. Hsu
Collaborators: (1.2:) Adil,(1.3:) Raahil, Marcos
Peer Reviewers: (A.4:) Adil, Alex, (1.2, 1.3:) Adil
Due Date: January 31, 2025

Appendix: Problem A.4.
Let $\varphi : S \to T$ be a surjective map between finite sets. Prove by induction that $|S| \geq |T|$ and that if $|S| = |T|$, then φ is bijective.

Proof. Let $\varphi : S \to T$ be a surjective map between finite sets. We prove by induction that $|S| \geq |T|$ and that if $|S| = |T|$, then φ is bijective.

Consider the base case when $|T| = 1$. Since φ is surjective, S must contain an element whose image is the single element $t \in T$. Thus, $|S| \geq 1$, and $|S| \geq |T|$.

For the inductive step, assume that the statement holds for any surjective map $\psi : S' \to T'$, where S' is the preimage of T' with $|T'| = k$. That is, we assume $|S'| \geq |T'|$, and if $|S'| = |T'|$, then ψ is bijective. Given that $|T'| = k$, we will now consider the case when $|T| = k + 1$ and prove that $|S| \geq |T|$.

Since φ is surjective, for every element in T there exists at least one preimage in S. Let $t \in T$, and define $T' = T - \{t\}$. By the surjectivity of φ, it follows that $S' = S - \{\varphi^{-1}(t)\}$, where S' contains all the elements in S mapping to t.

By the inductive hypothesis applied to the set $\varphi : S' \to T'$, we have $|S'| \geq |T'| = k$. Additionally, since $\{\varphi^{-1}(t)\} \neq \emptyset$, we have $|S| = |S'| + |\{\varphi^{-1}(t)\}| \geq k + 1 = |T|$. This establishes that $|S| \geq |T|$.

Additionally, let us suppose that $|S| = |T|$. Then from the previous argument, $|\{\varphi^{-1}(t)\}| = |\{t\}|$ and $|S'| = 1$. By the inductive hypothesis, φ is bijective. Since S' contains exactly one element mapping to t, it follows that φ is injective. Thus, with surjectivity, φ is bijective.

Indeed we conclude that $|S| \geq |T|$ for all finite sets S and T with a surjective map $\varphi : S \to T$, and that if $|S| = |T|$, then φ is bijective. $\square$

Chapter 2: Problem 1.2 *Prove the properties of inverses that are listed near the end of the section.*

- If an element a has both a left inverse l and a right inverse r, then $l = r$, a is invertible, and r is its inverse.
- If a is invertible, its inverse is unique.
- Inverses multiply in the opposite order: If a and b are invertible, so is the product ab, and $(ab)^{-1} = a^{-1}b^{-1}$.
- An element a may have a left inverse or a right inverse, though it is not invertible.

For the following properties, let us assume that we have a law of composition on a finite set S, where multiplication is defined as a binary operation $\cdot : S \times S \to S$, and a, r, and l are elements in S.

Proof. *Property 1*: Consider $ral = ral$, we will deduce that $r =$.

By commutativity, $(la)r = l(ar)$. And given that $la = 1$ and $ar = 1$, it is true that

$$\begin{aligned} (la)r &= l(ar) \\ 1r &= l1 \\ r &= l \end{aligned}$$

Thus, $l = r$ proving that a is invertible with inverse r.

Indeed, a is invertible given that a has a right inverse that is equal to its left inverse, where r is its inverse. □

Proof. *Property 2:* Let us assume that elements $b, c \in S$ are both inverses for invertible a in S.

By the definition of invertibility,

$$ba = ab = 1$$
$$\text{and}$$
$$ca = ac = 1$$

Due to the identity property, $ab = 1 = ac$. Thus, providing,

$$ab = ac$$

Given that c is assumed to be the inverse element of a,

$$\begin{aligned} ab &= ac \\ c(ab) &= c(ac) \\ b &= c \end{aligned}$$

Therefore, given two elements b and c that are both inverses to element a in S, they are evidently equal, proving the inverse to a is unique. □

Proof. Property 3: Let us assume that elements $a, b \in S$ are invertible. We shall prove that their product ab is also invertible with inverse $b^{-1}a^{-1}$.

$$(ab)(ab)^{-1} = 1$$

Since a is invertible, let its corresponding inverse be a^{-1}. Consequently,

$$\begin{gathered}(ab)(ab)^{-1} = 1 \\ (a^{-1})(ab)(ab)^{-1} = 1(a^{-1}) \\ (a^{-1}a)(b)(ab)^{-1} = a^{-1} \\ b(ab)^{-1} = a^{-1}\end{gathered}$$

Similarly, since b is also assumed invertible, let b have a corresponding inverse b^{-1} such that

$$\begin{gathered}b(ab)^{-1} = a^{-1} \\ (b^{-1})b(ab)^{-1} = (b^{-1})a^{-1} \\ (b^{-1}b)(ab)^{-1} = b^{-1}a^{-1} \\ 1(ab)^{-1} = b^{-1}a^{-1} \\ (ab)^{-1} = b^{-1}a^{-1}\end{gathered}$$

Thus, it is shown that given a and b to be invertible, their product ab is also invertible with the corresponding inverse shown as above. □

Proof. Property 4: Given that the property states that an element in a map may have a right or left inverse while not being invertible, an example of both cases of this property is sufficient for proof.

Consider the case where $s : \mathbb{N} \to \mathbb{N}$ is the shift map defined by $s(n) = n + 1$. The proof that this map results in solely a left inverse existing and a right inverse not existing is demonstrated in **problem 1.3** on the following page. Due to s not having both a left and a right inverse, the map is indeed not invertible. Thus, this problem is a valid example of the first half of the assumption.

Now we consider the case where an element may have only a right inverse and not a left inverse. That is, consider a map $r : \mathbb{N} \to \mathbb{N}$ defined as $r(n) = n + 1$, with an associated law of composition for two elements a and b described

$$a \circ b = b(a)$$

We shall first consider the right inverse of r which can be described as $t_r : \mathbb{N} \to \mathbb{N}$ defined

$$t_r(n) = n - 1, \text{for some natural number } n \geq 2.$$

Given our law of composition,

$$r(n) \circ t_r(n) = r(n) - 1 = n$$

Where $r(n) - 1 = n$ can be be alternatively written as,

$$r(n) = n + 1 \tag{1}$$

Equation (1) holds for all natural numbers (which we defined as such), thus the right inverse holds.

Let us consider the left inverse of r which can be described by

$$t_l(n) = n - 1, \text{for some natural number } n \geq 2.$$

Given our law of composition,

$$t_l \circ r(n) = t_l(n) + 1 = n. \tag{2}$$

Equation (2) holds true for all natural numbers $n \geq 2$; however, it poses a contradiction for the $n = 1$ case. For the $n = 1$ case,

$$t_l(1) + 1 = 1$$
$$t_l(1) = 0$$

However the conclusion that $t_l(1) = 0$ is a contradiction as our domain does not contain 0. Thus, since there is an element in the codomain of r that does not map to its corresponding domain $\mathbb{N}$, it must be true that there does not exist a left inverse function for r.

Thus, we were able to provide two sufficient examples that exemplify an element that has a corresponding left inverse without a right inverse, as well as an elemeent that has a corresponding right inverse without a left inverse. $\square$

Chapter 2: Problem 1.3

Let $\mathbb{N}$ denote the set $\{1, 2, 3, \dots\}$ of natural numbers, and let $s : \mathbb{N} \to \mathbb{N}$ be the shift map, defined by $s(n) = n + 1$. Prove that s has no right inverse, but that it has infinitely many left inverses.

Proof. Let $s(n) = n + 1$ be a mapped defined $s : \mathbb{N} \to \mathbb{N}$. We aim to prove that that s has no right inverse, but that s has infinitely many left inverses.

Let $t_l : \mathbb{N} \to \mathbb{N}$ be a left inverse function defined

$$t_l(n) = n - 1, \text{for some natural number } n \geq 2.$$

Given our law of composition,

$$t_l \circ s(n) = t_l(n + 1) = n. \tag{3}$$

It is true that equation (3) holds for all natural numbers $n \geq 2$. However, given that $t_l(1)$ does not map to from the codomain to our well-defined domain $\mathbb{N}$, it is then true that $t_l(1)$ can map to anything—subsequently having infinitely many inverses. Thus, there are infinite left inverses corresponding to s.

We shall now consider the right inverse function defined $t_r : \mathbb{N} \to \mathbb{N}$ where

$$t_r(n) = n - 1, \text{for some natural number } n \geq 2.$$

Similarly, the right inverse function composed with s can be simplified to

$$s \circ t_r(n) = t_r(n) + 1 = n. \tag{4}$$

Equation (4) holds true for all natural numbers $n \geq 2$; however, it poses a contradiction for the $n = 1$ case. For the $n = 1$ case,

$$\begin{gathered} t_r(1) + 1 = 1 \\ t_r(1) = 0 \end{gathered}$$

However the conclusion that $t_r(1) = 0$ is a contradiciton as our domain does not contain 0. Thus, since there is an element in the codomain of s that does not map to its corresponding domain $\mathbb{N}$, it must be true that there does not exist a right inverse function for s.

Indeed, we conclude that given the *shift* map $s : \mathbb{N} \to \mathbb{N}$ defined by $s(n) = n + 1$, s has no right inverse, but has infinitely many left inverses. $\square$