CS1231S: Discrete Structures

Tutorial #6: Functions

(Week 8: 7 – 11 October 2024)

Answers

---

1. Define the following relations on $\mathbb{N}$:

   $\forall x, y \in \mathbb{N}\ (x\ R_1\ y \ \Leftrightarrow x^2 = y^2)$;

   $\forall x, y \in \mathbb{N}\ (x\ R_2\ y \ \Leftrightarrow y \mid x)$;

   $\forall x, y \in \mathbb{N}\ (x\ R_3\ y \ \Leftrightarrow y = x + 1)$.

   Are the relations R_1, R_2 and R_3 functions? Prove or disprove.

   Answers:

   R_1 is a function.

   Proof:

   (F1) $\forall x \in \mathbb{N}, \exists y = x \in \mathbb{N}$ such that $(x, y) \in R_1$.

   (F2)
   1. $\forall x \in \mathbb{N}$, let $y_1, y_2 \in \mathbb{N}$.
   2. Suppose $(x, y_1) \in R_1 \wedge (x, y_2) \in R_1$.
   3. Then $y_1^2 = x^2$ and $y_2^2 = x^2$ (by the definition of R_1).
   4. Then $y_1^2 = y_2^2$.
   5. Hence $y_1 = y_2$ (as $y_1, y_2 \in \mathbb{N} \geq 0$).

   R_2 is not a function. Counterexample: $(6\ R_2\ 2) \wedge (6\ R_2\ 3)$.

   R_3 is a function.

   Proof:

   (F1) $\forall x \in \mathbb{N}, \exists y = x + 1 \in \mathbb{N}$ such that $(x, y) \in R_3$.

   (F2)
   1. $\forall x \in \mathbb{N}$, let $y_1, y_2 \in \mathbb{N}$.
   2. Suppose $(x, y_1) \in R_3 \wedge (x, y_2) \in R_3$.
   3. Then $y_1 = x + 1$ and $y_2 = x + 1$ (by the definition of R_3).
   4. Hence $y_1 = y_2$.

> A **function** $f: X \to Y$, is a relation satisfying the following properties:
> (F1) $\forall x \in X, \exists y \in Y$ such that $(x, y) \in f$.
> (F2) $\forall x \in X, \forall y_1, y_2 \in Y, \big((x, y_1) \in f \wedge (x, y_2) \in f\big) \to y_1 = y_2$.

2. Let $A = \{a, b\}$ and S be the set of all strings over A. (See Lecture 7 section 7.1.2 for the definition of string.)

Define a concatenate-by-a-on-the-left function $C: S \to S$ by $C(s) = as$ for all $s \in S$.

(a) Is C an injection? Prove or give a counterexample.

(b) Is C a surjection? Prove or give a counterexample.

Answers:

(a) Yes, C is an injection.

Proof:

1. Take any two strings $s_1, s_2 \in S$ and suppose $C(s_1) = C(s_2)$.
2. Then $as_1 = as_2$ by the definition of C.
   - 2.1. Let the length of as_1 and as_2 be n.
   - 2.2. Then the length of s_1 and s_2 is $n - 1$.
   - 2.3. Write $s_1 = x_1x_2 \cdots x_{n-1}$ and $s_2 = y_1y_2 \cdots y_{n-1}$ for $x_i, y_i \in A$, for all $i \in \{1,2,\cdots,n-1\}$.
   - 2.4. Thus $ax_1x_2 \cdots x_{n-1} = ay_1y_2 \cdots y_{n-1}$ by substitution.
   - 2.5. Thus $x_i = y_i$ for all $i \in \{1,2,\cdots,n-1\}$ by string equality.
   - 2.6. Hence $s_1 = s_2$.
3. Therefore C is an injection.

(b) No, C is not a surjection.

Proof:

1. Take the string b from S.
2. (Claim: There is no $s \in S$ such that $C(s) = b$.)
3. Suppose not, i.e., suppose $\exists s \in S$ such that $C(s) = b$.
   - 3.1. Then $C(s) = as = b$ by the definition of C.
   - 3.2. Then as and b have the same length.
   - 3.3. Since a and b have length 1, this means $s = \varepsilon$ (the empty string, which has a length of 0).
   - 3.4. But this means $b = as = a\varepsilon = a$.
   - 3.5. This is a contradiction since $a \neq b$.
4. Hence, for b, there is no $s \in S$ such that $C(s) = b$.
5. Therefore C is not a surjection.

3. Let $A = \{s, u\}$. Define a function $len: A^* \rightarrow \mathbb{Z}_{\geq 0}$ by setting $len(\sigma)$ to be the length of σ for each $\sigma \in A^*$.

(a) What is $len(suu)$?

(b) What is $len(\{\varepsilon, ss, uu, ssss\})$?

(c) What is $len^{-1}(\{3\})$?

(d) Does len^{-1} exist? Explain your answer.

Answers:

> **Theorem 7.2.3**
> If $f: X \rightarrow Y$ is a bijection, then $f^{-1}: Y \rightarrow X$ is also a bijection.
> In other words, $f: X \rightarrow Y$ is bijective iff f has an inverse.

(a) $len(suu) = 3$.

(b) $len(\{\varepsilon, ss, uu, ssss\}) = \{0,2,4\}$.

(c) $len^{-1}(\{3\}) = \{sss, ssu, sus, suu, uss, usu, uus, uuu\}$.

(d) $len(s) = 1 = len(u)$ but $s \neq u$. So len is not injective and so it is not bijective. Thus len^{-1} does not exist by Theorem 7.2.3. (Recall that len^{-1} refers to the inverse function of len.)

4. Given any two bijections $f: A \rightarrow B$ and $g: B \rightarrow C$, prove that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Answer:

1. Since f and g are bijections, f^{-1} and g^{-1} are bijections by theorem 7.2.3, and $g \circ f$ and $f^{-1} \circ g^{-1}$ are also bijection by theorems 7.3.3 and 7.3.4.
2. Since $g \circ f$ is a bijection, $(g \circ f)^{-1}$ exists and is a bijection by theorem 7.2.3.
3. (To check the domains and codomains of $(g \circ f)^{-1}$ and $f^{-1} \circ g^{-1}$.)
   3.1. Domain and codomain of $g \circ f$ are A and C respectively, hence domain and codomain of $(g \circ f)^{-1}$ are C and A respectively.
   3.2. Domain and codomain of f^{-1} are B and A respectively, domain and codomain of g^{-1} are C and B respectively, hence domain and codomain of $f^{-1} \circ g^{-1}$ are C and A respectively.
   3.3. Therefore, $(g \circ f)^{-1}$ and $f^{-1} \circ g^{-1}$ have the same domain and codomain.
4. (To check that $(g \circ f)^{-1}(z)$ and $f^{-1} \circ g^{-1}(z)$ have the same image for all $z \in C$.)
   4.1. Let $z \in C$.
   4.2 Then $\exists y \in B$ such that $z = g(y)$, or $y = g^{-1}(z)$ by definition of inverse function.
   4.3 Similarly, $\exists x \in A$ such that $y = f(x)$, or $x = f^{-1}(y)$ by definition of inverse function.
   4.4. Hence $(g \circ f)(x) = g\big(f(x)\big) = g(y) = z$, or $(g \circ f)^{-1}(z) = x$ by definition of inverse function.
   4.5 Also, $(f^{-1} \circ g^{-1})(z) = f^{-1}\big(g^{-1}(z)\big) = f^{-1}(y) = x$.
   4.6. Therefore, $(g \circ f)^{-1}(z) = f^{-1} \circ g^{-1}(z)$ for all $z \in C$ from lines 4.4 and 4.5.
5. Therefore, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ from 3 and 4.

> **Theorem 7.2.3**
> If $f: X \rightarrow Y$ is a bijection, then $f^{-1}: Y \rightarrow X$ is also a bijection.

> **Theorem 7.3.3**
> If $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are both injective, then $g \circ f$ is injective.

> **Theorem 7.3.4**
> If $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are both surjective, then $g \circ f$ is surjective.

5. Which of the functions defined in the following are injective? Which are surjective? Prove that your answers are correct. If a function defined below is both injective and surjective, then find a formula for the inverse of the function. Here we denote by $Bool$ the set {**true**, **false**}.

(a) $f: \mathbb{Q} \to \mathbb{Q}$;
$x \mapsto 12x + 31$.

(b) $g: Bool^2 \to Bool$;
$(p, q) \mapsto p \wedge {\sim} q$.

(c) $h: Bool^2 \to Bool^2$;
$(p, q) \mapsto (p \wedge q, p \vee q)$.

(d) $k: \mathbb{Z} \to \mathbb{Z}$;
$$x \mapsto \begin{cases} x, & \text{if } x \text{ is even;} \\ 2x - 1, & \text{if } x \text{ is odd.} \end{cases}$$

Inverse function
Let $f: X \to Y$. Then $g: Y \to X$ is an **inverse** of f iff
$\forall x \in X\ \forall y \in Y\ \big(y = f(x) \Leftrightarrow x = g(y)\big)$.

Answers:

(a) We could prove that f is injective and surjective, and hence bijective. Here, we try another approach: if we manage to find an inverse function for f, then by Theorem 7.2.3, f is bijective.

1. Note that for all $x, y \in \mathbb{Q}, y = 12x + 31 \Leftrightarrow x = (y - 31)/12$.
2. Define $f^*: \mathbb{Q} \to \mathbb{Q}$ by setting, for all $y \in \mathbb{Q}, f^*(y) = (y - 31)/12$.
3. Then whenever $x, y \in \mathbb{Q}, y = f(x) \Leftrightarrow x = f^*(y)$.
4. Thus f^* in the inverse of f.
5. Hence f is bijective (i.e. both injective and surjective) by Theorem 7.2.3.

(b)

1. $g(\mathbf{false}, \mathbf{true}) = \mathbf{false} = g(\mathbf{false}, \mathbf{false})$, where $(\mathbf{false}, \mathbf{true}) \neq (\mathbf{false}, \mathbf{false})$.
2. So g is not injective.
3. $g(\mathbf{true}, \mathbf{false}) = \mathbf{true}$.
4. Lines 1 and 3 show that every element of the codomain $Bool$ is in the range of g.
5. Hence g is surjective.

(c)

1. $h(\mathbf{true}, \mathbf{false}) = (\mathbf{false}, \mathbf{true}) = g(\mathbf{false}, \mathbf{true})$, where $(\mathbf{true}, \mathbf{false}) \neq (\mathbf{false}, \mathbf{true})$.
2. So h is not injective.
3. If $p, q, r \in Bool$ such that $h(p, q) = (\mathbf{true}, r)$, then
   3.1. $p \wedge q = \mathbf{true}$ by the definition of h;
   3.2. $\therefore p = \mathbf{true}$
   3.3. $\therefore r = p \vee q = \mathbf{true}$ by the definition of h.
4. So $(\mathbf{true}, \mathbf{false})$ in the codomain is not in the range of h.
5. Hence h is not surjective.

(d)

1. We first show that if x is an even integer, then $k(x)$ is even.
   1.1. Let x be an even integer.
   1.2. Then $k(x) = x$ by the definition of k.
   1.3. So $k(x)$ is even.

2. Next we show that if x is an odd integer, then $k(x)$ is odd.
   2.1. Let x be an odd integer.
   2.2. Then $k(x) = 2x - 1 = 2(x - 1) + 1$, where $x - 1$ is an integer.
   2.3. So $k(x)$ is odd.

3. Since every integer is either even or odd but not both, lines 1 and 2 tell us that, for every $x \in \mathbb{Z}$,
   3.1. x is even if and only if $k(x)$ is even; and
   3.2. x is odd if and only if $k(x)$ is odd.

4. Now we show that k is injective.
   4.1. Let $x_1, x_2 \in \mathbb{Z}$ such that $k(x_1) = k(x_2)$.
   4.2. Case 1: $k(x_1)$ is even.
      4.2.1. Then both x_1 and x_2 are even by line 3.1.
      4.2.2. So $x_1 = k(x_1) = k(x_2) = x_2$ by the definition of k.
   4.3. Case 2: $k(x_1)$ is odd.
      4.3.1. Then both x_1 and x_2 are odd by line 3.2.
      4.3.2. So $2x_1 - 1 = k(x_1) = k(x_2) = 2x_2 - 1$ by the definition of k.
      4.3.3. So $x_1 = x_2$.
   4.4. Since $k(x_1)$ is either even or odd, we conclude that $x_1 = x_2$ in any case.
   4.5. Therefore k is injective.

5. Finally, we prove by contradiction that k is not surjective.
   5.1. Suppose k is surjective.
   5.2. Note that 3 is in the codomain $\mathbb{Z}$.
   5.3. Use the surjectivity of k to find $x \in \mathbb{Z}$ such that $k(x) = 3$.
   5.4. Note that $k(x) = 3$ is odd and so x is odd by line 3.2.
   5.5. Thus $3 = k(x) = 2x - 1$ by the choice of x and the definition of k.
   5.6. Solving gives $x = \frac{3+1}{2} = 2$ which is even.
   5.7. This contradicts line 5.4 that x is odd.
   5.8. Therefore k is not surjective.

6. [AY2022/23 Semester 2 Exam Questions]
The following definitions are given.

Given a function $f: A \to B$, we say that
▪ $g: B \to A$ is a **left inverse** of f if and only if $g\big(f(a)\big) = a$ for all $a \in A$.
▪ $h: B \to A$ is a **right inverse** of f if and only if $f\big(h(b)\big) = b$ for all $b \in B$.

You do not need to provide proofs for the following parts.

(a) Which of the 4 functions given in question 5 have a left inverse?

(b) Which of the 4 functions given in question 5 have a right inverse?

(c) Which of the following statements are true?

(i) If a function has a left inverse, then it has a right inverse.

(ii) If a function has a right inverse, then it has a left inverse.

Answers:

(a) Only f and k. (b) Only f and g. (c) Neither is true.

Note that

- a function is injective if and only if it has a left inverse;
- a function is surjective if and only if it has a right inverse.

7. We have shown in Theorem 7.3.3 that if $f: X \to Y$ and $g: Y \to Z$ are both injective, then $g \circ f$ is injective.

Now, let $f: B \to C$. Suppose we have a function g with domain C such that $g \circ f$ is injective. Show that f is injective.

Answer:

1. Suppose g is a function with domain C such that $g \circ f$ is injective.
2. Let $x_1, x_2 \in B$ such that $f(x_1) = f(x_2)$.
3. Then $(g \circ f)(x_1) = g\big(f(x_1)\big) = g\big(f(x_2)\big) = (g \circ f)(x_2)$ by the definition of $g \circ f$.
4. So $x_1 = x_2$ as $g \circ f$ is injective by the choice of g.
5. Therefore f is injective.

8. Let $A = \{1,2,3\}$. The ***order*** of a bijection $f: A \to A$ is defined to be the smallest $n \in \mathbb{Z}^+$ such that

$$\underbrace{f \circ f \circ \cdots \circ f}_{n\text{-many } f\text{'s}} = id_A.$$

Define functions $g, h: A \to A$ by setting, for all $x \in A$,

$$g(x) = \begin{cases} 1, & \text{if } x = 2; \\ 2, & \text{if } x = 1; \\ x, & \text{otherwise,} \end{cases} \qquad h(x) = \begin{cases} 2, & \text{if } x = 3; \\ 3, & \text{if } x = 2; \\ x, & \text{otherwise.} \end{cases}$$

Find the orders of $g, h, g \circ h$, and $h \circ g$.

Answers: The orders for $g, h, g \circ h$, and $h \circ g$ are 2, 2, 3 and 3 respectively.

$(g \circ g)(1) = g\big(g(1)\big) = g(2) = 1$
$(g \circ g)(2) = g\big(g(2)\big) = g(1) = 2$
$(g \circ g)(3) = g\big(g(3)\big) = g(3) = 3$
Therefore $g \circ g$ is an identity function on A. Hence $g \circ g$ has an order of 2.

Similar working for h.

Let $s = g \circ h$.
$s(1) = (g \circ h)(1) = g\big(h(1)\big) = g(1) = 2$
$s(2) = (g \circ h)(2) = g\big(h(2)\big) = g(3) = 3$
$s(3) = (g \circ h)(3) = g\big(h(3)\big) = g(2) = 1$
$(s \circ s \circ s)(1) = s\Big(s\big(s(1)\big)\Big) = s\big(s(2)\big) = s(3) = 1$
$(s \circ s \circ s)(2) = s\Big(s\big(s(2)\big)\Big) = s\big(s(3)\big) = s(1) = 2$
$(s \circ s \circ s)(3) = s\Big(s\big(s(3)\big)\Big) = s\big(s(1)\big) = s(2) = 3$
Therefore $(g \circ h) \circ (g \circ h) \circ (g \circ h)$ is an identity function on A. Hence $g \circ h$ has an order of 3.

Similar working for $h \circ g$.

9. Let $f: A \to B$ be a function. Let $X \subseteq A$ and $Y \subseteq B$. Justify your answers for the following:

(a) Is it always the case that $X \subseteq \boldsymbol{f}^{-1}(\boldsymbol{f}(X))$? Is it always the case that $\boldsymbol{f}^{-1}(\boldsymbol{f}(X)) \subseteq X$?

(b) Is it always the case that $Y \subseteq \boldsymbol{f}\left(\boldsymbol{f}^{-1}(Y)\right)$? Is it always the case that $\boldsymbol{f}\left(\boldsymbol{f}^{-1}(Y)\right) \subseteq Y$?

Note that $\boldsymbol{f}(X)$ is the **(setwise) image** of X, and $\boldsymbol{f}^{-1}(Y)$ the **(setwise) preimage** of Y under f, where $X \subseteq A$ and $Y \subseteq B$. Without the colored font to disambiguate the two kinds of functions, it should also be clear what $f(U)$ denotes, depending on whether $U \in A$ or $U \in P(A)$.

> Let $f: X \to Y$ be a function from set X to set Y.
> - If $A \subseteq X$, then let $\boldsymbol{f}(A) = \{f(x) : x \in A\}$.
> - If $B \subseteq Y$, then let $\boldsymbol{f}^{-1}(B) = \{x \in X : f(x) \in B\}$
>
> We call $\boldsymbol{f}(A)$ the **(setwise) image** of A, and $\boldsymbol{f}^{-1}(B)$ the **(setwise) preimage** of B under f.

Answers:

(a) First, we show it is always the case that $X \subseteq f^{-1}(f(X))$.

1. Let $x \in X$.
2. Then $f(x) \in f(X)$ by the definition of $f(X)$.
3. So $x \in f^{-1}(f(X))$ by the definition of $f^{-1}(f(X))$.

Next, we show it is possible that $f^{-1}(f(X)) \nsubseteq X$.

1. Consider $f: \{-1,1\} \to \{0\}$ where $f(-1) = 0 = f(1)$, and $X = \{1\}$.
2. Note that $f(X) = \{f(1)\} = \{0\}$.
3. Since $f(-1) = 0$, we know $-1 \in f^{-1}(\{0\}) = f^{-1}(f(X))$.
4. As $-1 \notin \{1\} = X$, we deduce that $f^{-1}(f(X)) \nsubseteq X$.

(Other counterexamples are possible.)

(b) First, we show it is always the case that $f(f^{-1}(Y)) \subseteq Y$.

1. Take any $y \in f(f^{-1}(Y))$.
2. Then we have some $x \in f^{-1}(Y)$ such that $y = f(x)$, by the definition of $f(f^{-1}(Y))$.
3. Now, as $x \in f^{-1}(Y)$, we get $y' \in Y$ which makes $y' = f(x)$.
4. Since f is a function, this implies $y = f(x) = y' \in Y$ as required.

Next, we show it is possible that $Y \nsubseteq f(f^{-1}(Y))$? .

1. Consider $f: \{0\} \to \{-1,1\}$ where $f(0) = 1$, and $Y = \{-1\}$.
2. Note that no $x \in \{0\}$ makes $f(x) = -1$.
3. So $f^{-1}(Y) = \emptyset$ by the definition of $f^{-1}(Y)$.
4. This entails $f(f^{-1}(Y)) = \emptyset \nsupseteq \{-1\} = Y$.

(Other counterexamples are possible.)

10. Consider the equivalence relation $\sim$ on $\mathbb{Q}$ defined by setting, for all $x, y \in \mathbb{Q}$,

$$x \sim y \Leftrightarrow x - y \in \mathbb{Z}.$$

Define addition and multiplication on $\mathbb{Q}/\sim$ as follows: whenever $[x], [y] \in \mathbb{Q}/\sim$,

$$[x] + [y] = [x + y] \quad \text{and} \quad [x] \cdot [y] = [x \cdot y].$$

(a) Is $+$ well defined on $\mathbb{Q}/\sim$?

(b) Is $\cdot$ well defined on $\mathbb{Q}/\sim$?

Prove that your answers are correct.

> **Lemma Rel.1 Equivalence Classes**
> Let $\sim$ be an equivalence relation on a set A. The following are equivalent for all $x, y \in A$.
> (i) $x \sim y$; (ii) $[x] = [y]$; (iii) $[x] \cap [y] \neq \emptyset$.

Answers:

(a) We claim that $+$ is well defined on $\mathbb{Q}/\sim$.

1. Let $[x_1], [y_1], [x_2], [y_2], \in \mathbb{Q}/\sim$ such that $[x_1] = [x_2]$ and $[y_1] = [y_2]$.
2. So $x_1 \sim x_2$ and $y_1 \sim y_2$ by Lemma Rel.1.
3. Use the definition of $\sim$ to find $k, l \in \mathbb{Z}$ such that $x_1 - x_2 = k$ and $y_1 - y_2 = l$.
4. Note that $(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2) = k + l \in \mathbb{Z}$.
5. So $x_1 + y_1 \sim x_2 + y_2$ by the definition of $\sim$.
6. Hence $[x_1] + [y_1] = [x_1 + y_1] = [x_2 + y_2] = [x_2] + [y_2]$ by Lemma Rel.1.

(b) We claim that $\cdot$ is not well defined on $\mathbb{Q}/\sim$.

1. Note that $\frac{1}{2} - \frac{-1}{2} = 1 \in \mathbb{Z}$.
2. This implies $\frac{1}{2} \sim \frac{-1}{2}$ and so $\left[\frac{1}{2}\right] = \left[\frac{-1}{2}\right]$ by Lemma Rel.1.
3. Note that $\frac{1}{4} - \frac{-1}{4} = \frac{1}{2} \notin \mathbb{Z}$.
4. This implies $\frac{1}{4} \nsim \frac{-1}{4}$ and so $\left[\frac{1}{4}\right] \neq \left[\frac{-1}{4}\right]$ by Lemma Rel.1.
5. Therefore, according to the definition of $\cdot$ on $\mathbb{Q}/\sim$,

$$\left[\frac{1}{2}\right] \cdot \left[\frac{1}{2}\right] = \left[\frac{1}{2} \cdot \frac{1}{2}\right] = \left[\frac{1}{4}\right] \neq \left[\frac{-1}{4}\right] = \left[\frac{1}{2} \cdot \frac{-1}{2}\right] = \left[\frac{1}{2}\right] \cdot \left[\frac{-1}{2}\right].$$

11. Consider the addition function + under $\mathbb{Q}$.

Consider a new function $+$ you constructed in Q10 for addition on $\mathbb{Q}/\sim$ as follows:

whenever $[x], [y] \in \mathbb{Q}/\sim$, we have $[x] + [y] = [x + y]$.

The type signature for function + under $\mathbb{Q}$ would be:

$+ : (\mathbb{Q}, \mathbb{Q}) \rightarrow \mathbb{Q}$

What is the type signature of the new function $+$ which you just constructed via the above equality relation?

Answer:

$+ : (\mathbb{Q}/\sim, \mathbb{Q}/\sim) \rightarrow \mathbb{Q}/\sim$