Chapter 7

[7] Properties of Functions

[7.1] Functions Defined on General Sets

- This chapter will restate previous definitions from Chapter 1 with additional terminology
- A **function** f from set X to set Y is denoted as $X \to Y$
  - Also known as the relation from f's **domain** X to f's **co-domain** Y
  1. Every element in X is related to some element in Y
  2. No element in X is related to more than one element in Y
- Thus, any element $x \in X$ sends/maps to a unique value $y \in Y$
- This is denoted as $x \xrightarrow{f} y$ or $f\colon x \to y$
- y is denoted as $f(x)$, read f of x or
  - The output of f for the input x
  - The value of f at x
  - The image of f under x
- The set of all values of f is known as **the range of** f or **the image of** X **under** f
  - Symbolically:

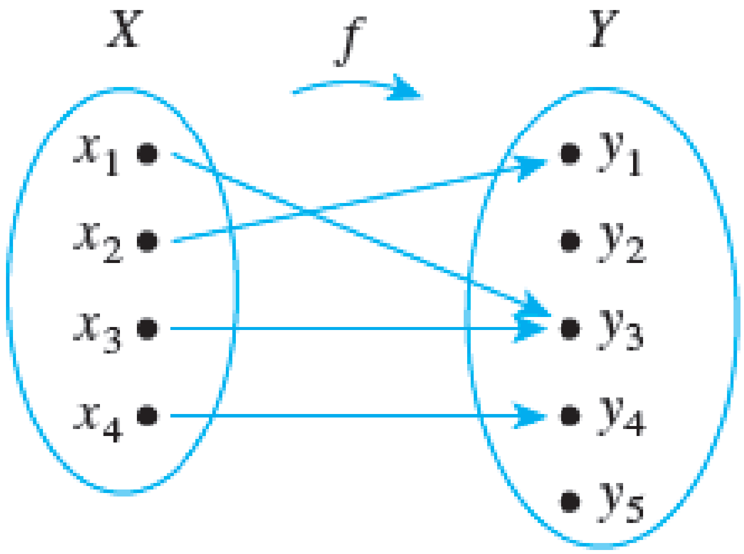
$$f = \{\, x \in X \mid f(x) = y \,\}$$

- x is **the preimage of** y or **an inverse image of** y if it results in an image of y
- The set of all values of all inverse images of y is the **inverse image of** y
  - Symbolically:

$$\text{inverse image of } y = \{\, x \in X \mid f(x) = y \,\}$$

Arrow Diagrams

- If X and Y are finite sets, then f may be defined between X and Y with an arrow diagram, showing a single mapping from each $x \in X$ to a unique $y \in Y$



  - The domain $\{x_1, x_2, x_3, x_4\}$ mapping onto the co-domain $\{y_1, y_2, y_3, y_4, y_5\}$
  - The range of f is $\{y_1, y_3, y_4\}$
  - The inverse image of y_3 is $\{x_1, x_2\}$
  - The inverse image of y_2 is $\varnothing$
  - As a set of ordered pairs, this set is $\{(x_1, y_3), (x_2, y_1), (x_3, y_3), (x_4, y_4)\}$
- **Theorem 7.1.1:** A test for function equality
  - If $F\colon\ X \to Y$ and $G\colon X \to Y$ are functions, then $F = G$ if, and only if, $F(x) = G(x)$ for every $x \in X$
- Ex: If $F\colon \mathbb{R} \to \mathbb{R}$ and $G\colon \mathbb{R} \to \mathbb{R}$, are $F + G\colon \mathbb{R} \to \mathbb{R}$ and G:

Examples of Functions

- An **identity function** is a function whose output is the same as the input
  - Below is the identity function on X

$$I_X(x) = x \quad \text{for each } x \text{ in } X.$$

- **Infinite sequences** are formally defined as functions on the set of all integers all greater than or equal to a particular integer

$$1, -\frac{1}{2}, \frac{1}{3}, -\frac{1}{4}, \frac{1}{5}, \ldots, \frac{(-1)^n}{n+1}$$

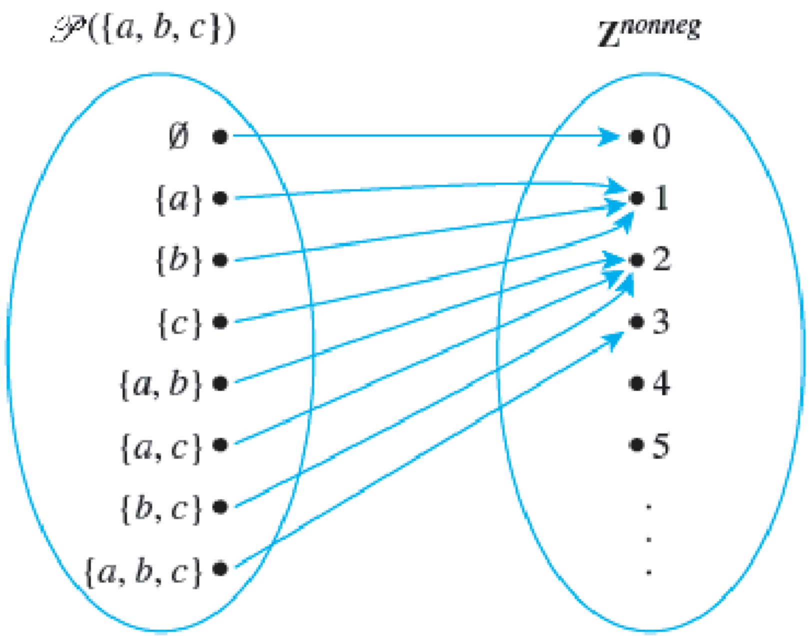
  - Infinite sequences can be defined by numerous functions with different input sets

- In this case, different rules can be found for $f\colon \mathbb{N} \to \mathbb{R}$ and $g\colon \mathbb{Z}^+ \to \mathbb{R}$

$$\text{Map each integer } n \geq 0 \text{ using } f(n) = \frac{(-1)^n}{n+1}$$

$$\text{Map each integer } n \geq 1 \text{ using } g(n) = \frac{(-1)^{n+1}}{n}$$

- **Functions defined on power sets** whose output is the number of elements for each $X \in \mathcal{P}(X)$
  - Thus, $F\colon \mathcal{P}(X) \to \mathbb{N}$



- **Functions defined on cartesian products** are functions who map a cartesian product input to an output
  - $M\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ and $R\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$

$$M(a,b) = ab \quad \text{and} \quad R(a,b) = (-a,b)$$

  - *For formatting reasons, the parentheses for the cartesian product is implicit*
- **Definition logarithms** and **logarithmic functions** are functions whose output is the exponent the logarithmic base needs to be raised to in order to equal the input
  - $L\colon \mathbb{R}^+ \to \mathbb{R}$

$$\log_b x = y \iff b^y = x$$

- **Strings** are finite sequences of elements that may wrap over a function with a **length** equal to the number of characters

Boolean Functions

- **Boolean functions** are functions with a domain containing all ordered n-tuples of 0s and 1s with a co-domain $\{0,1\}$
  - *Essentially, the domain is the Cartesian product of* n *copies of* $\{0,1\}$*, denoted* $\{0,1\}^n$
  - $f: \{0,1\}^n \to \{0,1\}$
- They are represented as tables and as arrow diagrams
- Ex: Given $f(x_1, x_2, x_3) = (x_1 + x_2 + x_3) \bmod 2$

x_1	x_2	x_3	$(x_1 + x_2 + x_3) \bmod 2$
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	1
0	0	0	0

Checking Whether a Function is Well Defined

- Functions are **not well defined** if it fails to satisfy the defining requirements of being a function
- Ex: $f\left(\frac{m}{n}\right) f = m$ for all integers m and n with $n \neq 0$
  - This function is not defined because fractions have multiple quotient representations, thus equivalent fractions may yield different values because they have different numerators

$$\frac{1}{2} = \frac{3}{6}$$

$$f\left(\frac{1}{2}\right) = 1$$
$$f\left(\frac{3}{6}\right) = 3$$

$$f\left(\frac{1}{2}\right) \neq f\left(\frac{3}{6}\right)$$

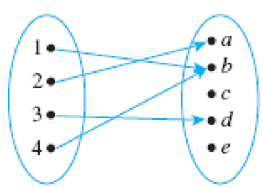
- However, a well defined function literally means that it can be called a function

Functions Acting on Sets

- In a function defined from set X to set Y, the set of all images in Y is a subset of the set of all images of X, and the set of all inverse images in X is a subset of Y
- If $f\colon X \to Y$ is a function and $A \subseteq X$ and $C \subseteq Y$, then

$$f(A) = \{\, y \in Y \mid y = f(x) \quad \text{for some } x \text{ in } A \,\}$$
$$\text{and}$$
$$f^{-1}(C) = \{\, x \in X \mid f(x) \in X \,\}$$

  - where $f(A)$ is **the image of** A and $f^{-1}(C)$ is the **inverse image of** C
- Ex: Let $X = \{\, 1, 2, 3, 4 \,\}$ and $Y = \{\, a, b, c, d, e \,\}$, and define $F\colon X \to Y$ using the following diagram



  - Additionally, let $A = \{\, 1, 4 \,\}$, $C = \{\, a, b \,\}$, and $D = \{\, c, e \,\}$
  - Evaluate F using different sets

$$F(A) = \{\, b \,\}$$
$$F(X) = \{\, a, b, d \,\}$$
$$F^{-1}(C) = \{\, 1, 4 \,\}$$
$$F^{-1}(D) = \varnothing$$

- Ex: Let X and Y be sets, let F be a function from X to Y, and let A and B be any subsets of X. Prove

$$F(A \cup B) \subseteq F(A) \cup F(B)$$

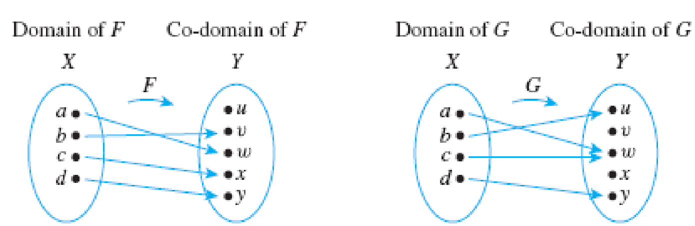
  - Suppose $y \in F(A \cup B)$
  - By definition of F, $y = F(x)$ for some $x \in A \cup B$
  - By definition of union, $x \in A \vee x \in B$
  - **Case 1:** $x \in A$
    - By definition of F, $y \in F(A)$
    - By definition of union, $y \in F(A) \cup F(B)$
  - **Case 2:** $x \in B$
    - By definition of F, $y \in F(B)$
    - By definition of union, $y \in F(A) \cup F(B)$
  - In both cases, $y \in F(A) \cup F(B)$, so the given statement is true

▼ [7.2] One-to-One, Onto, and Inverse Functions

One-to-One Functions

- If no two elements in the domain map onto the same element in the co-domain, then the function if **one-to-one** or **injective**
  - Thus, every element in the co-domain is the image of at most one element in the domain
  - Symbolically,

$$F\colon X \to Y \text{ is } \textbf{one-to-one} \iff \forall x_1, x_2 \in X, \\ F(x_1) = F(x_2) \implies x_1 = x_2$$



One-to-One Functions on Infinite Sets

- For proving that a function is one-to-one on infinite sets, suppose that x_1 and x_2 are elements of X such that $f(x_1) = f(x_2)$, then show that $x_1 = x_2$

- On the other hand, to disprove a function being one-to-one, show an example such that $f(x_1) = f(x_2)$ and $x_1 \neq x_2$

$$F\colon X \to Y \text{ is not } \textbf{one-to-one} \iff \exists x_1, x_2 \in X, \\ F(x_1) = F(x_2) \land x_1 \neq x_2$$

- Ex: $f\colon \mathbb{R} \to \mathbb{R}$ is defined as

$$f(x) = 4x - 1 \quad \text{for each real number } x$$

  - Suppose x_1 and x_2 are real numbers such that

$$f(x_1) = f(x_2)$$

  - *Show* $x_1 = x_2$

$$4x_1 - 1 = 4x_2 - 1 \tag{i}$$
$$4x_1 = 4x_2 \tag{ii}$$
$$x_1 = x_2 \tag{iii}$$

    - (i) → By substitution
    - (ii) → By adding 1
    - (iii) → By dividing by 4
  - Thus, the given statement is true

Application: Hash Functions

- A **hash function** is a function defined from a larger, possibly infinite, set of data to a smaller fixed-size set of integers
- They are defined using mod functions and using prime numbers to prevent clustering
- They are one-to-one, and the co-domain should be much larger than the domain
  - It is still possible for input values to **collide**, causing a **collision**, handled using **collision resolution methods**
- For example, let hash function H be a function from the set of all student ID numbers to the set $\{0, 1, 2, 3 \ldots, 10\}$

$$H(n) = n \bmod 11 \quad \text{for each ID number } n$$

  - Notably, if H is to be one-to-one, it is very unreliable because there are many possibly students IDs that may yield the hash code

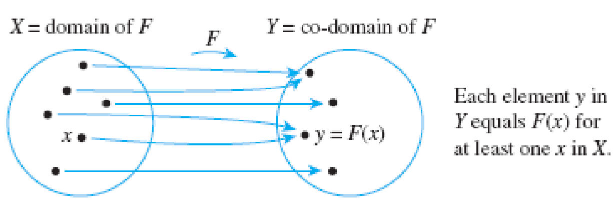
- Thus, it could implement **linear probing** if a collision occurs where it checks every successive hash code until it finds an available one

- **Cryptographic hash functions** are hash functions satisfying two particular conditions
  1. It is a function from bit strings to bit strings of fixed length
  2. It is close to being one-to-one
     a. *Low chance of collisions*
  3. It is close to being one-way
     a. *For any bit in its range, finding the string's inverse image is difficult to compute*
  4. The hash computation is quick
  5. Slight changes in input string leads to extensive changes in the output string
- Cryptographic hash functions are most popular for password security
  - Instead of storing company passwords as clear text, for example, they apply a cryptographic hash function to each or to a group of passwords, storing the resulting **hashes**
- Thus, checking equality is done by applying the hash function to the input and comparing the hashes
- Other applications include file copying, file transmissions, and the blockchain

Onto Functions

- If all elements in the co-domain are the image of an element in the domain, then the function is **onto** or **surjective**
  - Symbolically,

$$F\colon X \to Y \text{ is } \textbf{onto} \iff \forall y \in Y, \exists x \in X, \\ \text{such that } F(x) = y$$



Onto Functions on Infinite Sets

- For proving that a function is onto on infinite sets, suppose that y is any element of Y , then show that there is an element x in X such that $F(x) = y$
- On the other hand, to disprove a function being onto, show an example such that $y \neq F(x)$ for any x in X

$$F\colon X \to Y \text{ is not } \textbf{onto} \iff \exists y \in Y \text{ such that } \forall x \in X,\, F(x) \neq y$$

- Ex: $f\colon \mathbb{R} \to \mathbb{R}$ defined as

$$f(x) = 4x - 1 \quad \text{for each real number } x$$

  - Suppose y is a real number
  - Let $x = (y + 1) \div 4$
  - x is a real number because $\mathbb{R}$ is closed under addition and division

$$\begin{aligned} y &= f(x) \\ &= f\left(\frac{y+1}{4}\right) && \text{(i)} \\ &= 4\left(\frac{y+1}{4}\right) - 1 && \text{(ii)} \\ &= y + 1 - 1 && \text{(iii)} \\ &= y && \text{(iii)} \end{aligned}$$

    - (i) → By substitution
    - (ii) → By definition of f
    - (iii) → By algebra
  - Thus, the given statement is true
- Ex: $h\colon \mathbb{Z} \to \mathbb{Z}$ defined as

$$h(n) = 4n - 1 \quad \text{for each integer } n$$

  - *Notice how if $h(n)$ can be represented by $\mathbb{Z}$, then n may not always be an integer because it must satisfy the requirement $n \bmod 4 = 3$, which not all integers do*
  - A counterexample is $h(n) = 0$

$$\begin{aligned} 4n - 1 &= 0 && \text{(By substitution)} \\ 4n &= 1 && \text{(By adding 1)} \\ n &= \frac{1}{4} && \text{(Dividing by 4)} \end{aligned}$$

  - $\frac{1}{4}$ is not an integer, hence there is no integer n for which $h(n) = 0$
  - Therefore, h is not an onto function

Relationships between Exponential and Logarithmic Functions

- **Definition logarithms** and **logarithmic functions** are functions whose output is the exponent the logarithmic base needs to be raised to in order to equal the input
- **Exponential functions** are functions whose output is the power base b will be raised to
  - $b \neq 1$
  - $\exp_b\colon \mathbb{R} \to \mathbb{R}^+$

$$\exp_b(x) = b^x$$

- Laws of exponents given positive real numbers b and c and real numbers u and v

$$\begin{aligned} b^u b^v &= b^{u+v} \\ (b^u)^v &= b^{uv} \\ \frac{b^u}{b^v} &= b^{u-v} \\ (bc)^u &= b^u c^u \end{aligned}$$

- Notice how logarithmic functions are defined opposite that of exponential functions, being from $\mathbb{R}^+$ to $\mathbb{R}$ and having the resultant simplified exponent as the input and the power as the output

$$\log_b x = y \iff b^y = x$$

- Logically, logarithmic functions and exponential functions are both one-to-one and onto

$$\begin{aligned} b^u = b^v &\implies u = v \\ \log_b u = \log_b v &\implies u = v \end{aligned}$$

- **Theorem 7.2.1:** Properties of logarithms
  - For any positive real numbers b, c, x, and y for $b \neq 1$ and $c \neq 1$ and $\forall$ real number a

$$\begin{aligned} \log_b(xy) &= \log_b x + \log_b y \\ \log_b\left(\frac{x}{y}\right) &= \log_b x - \log_b y \\ \log_b(x^a) &= a \log_b x \\ \log_c x &= \frac{\log_b x}{\log_b c} \end{aligned}$$

- Ex: Prove the following logarithmic property

$$\log_c x = \frac{\log_b x}{\log_b c}$$

- Suppose positive real numbers b, c, and x are given for $b \neq 1$ and $c \neq 1$
- Let

$$u = \log_b c \tag{1}$$
$$v = \log_c x \tag{2}$$
$$w = \log_b x \tag{3}$$

- By definition of logarithms,

$$c = b^u \tag{1'}$$
$$x = c^v \tag{2'}$$
$$x = b^w \tag{3'}$$

- *Using these equalities, we can derive the property using exponent laws*

$$\begin{aligned} x &= c^v && \text{(i)} \\ &= (b^u)^v && \text{(ii)} \\ &= b^{uv} && \text{(iii)} \end{aligned}$$

$$\begin{aligned} b^{uv} &= b^w && \text{(i)} \\ uv &= w && \text{(iv)} \\ (\log_b c)(\log_c x) &= \log_b x && \text{(v)} \\ \log_c x &= \frac{\log_b x}{\log_b c} && \text{(vi)} \end{aligned}$$

  - (i) → By substitution from 2′
  - (ii) → By substitution from 1′
  - (iii) → By laws of exponents
  - (iv) → By one-to-oneness of exponential functions
  - (v) → By substitution from 1, 2, and 3
  - (vi) → By algebra
- $\log_b c$ is not zero because $b \neq 0$
- Thus, the property has been proven

One-to-One Correspondences

- A **one-to-one correspondence** or **bijection** exists from a set X to a set Y is a function between them that is one-to-one and onto

- For instance, given a power set of $\{ a, b \}$ and a bit string S, a function h with one-to-one correspondence can be defined between them with the rule
  - 1 corresponds to a and b in the first and second position respectively
  - 0 corresponds to anything else

$$\begin{pmatrix} \mathcal{P}(\{ a, b \}) \\ \varnothing \\ \{ a \} \\ \{ b \} \\ \{ a, b \} \end{pmatrix} \begin{matrix} \xrightarrow{h} \\ \rightarrow \\ \rightarrow \\ \rightarrow \\ \rightarrow \end{matrix} \begin{pmatrix} S \\ \{ 0, 0 \} \\ \{ 1, 0 \} \\ \{ 0, 1 \} \\ \{ 1, 1 \} \end{pmatrix}$$

  - h is onto because every element in S corresponds to an element in $\mathcal{P}(\{ a, b \})$
  - h is one-to-one because every element in $\mathcal{P}(\{ a, b \})$ has a distinct output when mapped using h
  - Thus, h is a one-to-one correspondence
- As seen in previous example, arrow diagrams clearly indicate one-to-one correspondences by showing arrows forming distinct element pairs between the sets
- Ex: Given F: $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$ defined by the rule

$$F(x, y) = (3y - 1, 1 - x)$$

  - Prove that F is a one-to-one correspondence
  - **Part 1:** Prove that F is one-to-one
    - Suppose x_1, y_1, x_2, y_2 are real numbers such that

$$F(x_1, y_1) = F(x_2, y_2)$$

    - Left side of the tuple

$$\begin{aligned} 3y_1 - 1 &= 3y_2 - 1 && \text{(i)} \\ 3y_1 &= 3y_2 && \text{(ii)} \\ y_1 &= y_2 && \text{(iii)} \end{aligned}$$

      - (i) → By substitution
      - (ii) → By adding 1 to both sides
      - (iii) → By dividing by 3 on both sides
    - Right side of the tuple

$$\begin{aligned} 1 - x_1 &= 1 - x_2 && \text{(i)} \\ -x_1 &= -x_2 && \text{(ii)} \\ x_1 &= x_2 && \text{(iii)} \end{aligned}$$

- (i) → By substitution
- (ii) → By subtracting 1 from both sides
- (iii) → By dividing both sides by -1

- By definition of tuple, $(x_1, y_1) = (x_2, y_2)$
- Therefore, F is one-to-one

- **Part 2:** Prove that F is onto
  - Suppose that (u, v) is any tuple in $\mathbb{R} \times \mathbb{R}$
  - *Let x and y be any expression in terms of u or v that will eventually simplify to (u, v) when mapped using F*
  - Let $x = 1 - v$ and $y = \frac{1}{3}u + \frac{1}{3}$
  - Thus,

$$\begin{aligned} F(x, y) &= F\left(1 - v, \frac{1}{3}u + \frac{1}{3}\right) && \text{(i)} \\ &= \left(3\left(\frac{1}{3}u + \frac{1}{3}\right) - 1, 1 - (1 - v)\right) && \text{(ii)} \\ &= (u + 1 - 1, 1 - 1 + v) && \text{(iii)} \\ &= (u, v) && \text{(iv)} \end{aligned}$$

- (i) → By substitution
- (ii) → By definition of F
- (iii) → By distributive property
- (iv) → By algebra

  - Therefore, F is onto
- Because F is one-to-one and onto, it is also a one-to-one correspondence

Inverse Functions

- An **inverse function** of a function maps an element of the original function’s co-domain onto its preimage in the domain
  - *For a function F, the inverse is denoted as F^{-1}*

- **Theorem 7.2.2:**

$$F^{-1}(y) = x \iff y = F(x)$$

- For instance, logarithmic and exponential functions are inverses of each other
- Logically, inverse functions may only exist for functions which are one-to-one correspondences
- Using the previous arrow diagram of h between the power set and the bit string, the mapping just has to be flipped; taking S as the domain and the corresponding subsets as the range/domain

$$\begin{pmatrix} \mathcal{P}(\{a,b\}) \\ \varnothing \\ \{a\} \\ \{b\} \\ \{a,b\} \end{pmatrix} \begin{matrix} \xleftarrow{h^{-1}} \\ \leftarrow \\ \leftarrow \\ \leftarrow \\ \leftarrow \end{matrix} \begin{pmatrix} S \\ \{0,0\} \\ \{1,0\} \\ \{0,1\} \\ \{1,1\} \end{pmatrix}$$

- Ex: Find the inverse of the one-to-one correspondence $f\colon \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = 4x - 1 \quad \text{for each real number } x$$

  - For any *particular but arbitrarily chosen* y in $\mathbb{R}$, by definition of inverse function, $f^{-1}(y) = x$ for each real number x such that $f(x) = y$

$$\begin{aligned} f(x) &= y \\ 4x - 1 &= y && \text{(i)} \\ 4x &= y + 1 && \text{(ii)} \\ x &= \frac{y+1}{4} && \text{(ii)} \\ f^{-1}(y) &= \frac{y+1}{4} && \text{(iii)} \end{aligned}$$

    - (i) → By definition of f
    - (ii) → By algebra
    - (iii) → By definition of f^{-1}

- Ex: Define the inverse function $F^{-1}\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ for the following one-to-one correspondence

$$F\left(\frac{u+v}{2}, \frac{u-v}{2}\right) = (u, v)$$

- *Because F is one-to-one, we know that input is a unique ordered pair mapped by the function to (u, v)*
- Thus,

$$F^{-1}(u, v) = \left(\frac{u+v}{2}, \frac{u-v}{2}\right)$$

- **Theorem 7.2.3:**
  - If X and Y are sets and $F: X \to Y$ is onto and one-to-one, then $F^{-1}: Y \to X$ is also onto and one-to-one

▼ [7.3] Composition of Functions

- The output of one function may be used as the input of another function
  - This is known as **composing** functions
- Composition of functions only works if the first function's range is contained in the second function's domain
- Let $f: X \to Y$ and g be a function from Y' to Z; a new function $g \circ f: X \to Z$ may be defined as follows

$$(g \circ f)(x) = g\big(f(x)\big) \quad \text{for each } x \in X$$

  - and is known as the **composition of f and g**
  - *Where $g \circ f$ is read as "g circle f" and $g\big(f(x)\big)$ is read as "g of f of x." While the former may refer to the name of a composition function, the latter refers to its value at x*
- Arrow diagrams can represent composition functions with three sets representing each function
  - The leftmost set is the domain of the composition, and the rightmost set is the range of the composition
- Ex: Given $f: \mathbb{Z} \to \mathbb{Z}$ and $g: \mathbb{Z} \to \mathbb{Z}$ defined as

$$\begin{aligned} &f(n) = n + 1 \\ &g(n) = n^2 \\ &\text{for each } n \in \mathbb{Z} \end{aligned}$$

  - the compositions $f \circ g$ and $g \circ f$ are defined as follows

$$\begin{aligned} (f \circ g)(n) &= f\big(g(n)\big) = \left(n^2\right) + 1 = n^2 + 1 \\ (g \circ f)(n) &= g\big(f(n)\big) = (n+1)^2 = n^2 + 2n + 1 \end{aligned}$$

- *Notice how for f and g, the order of the composition matters as the resulting functions clearly yield different values for some inputs*

$$(f \circ g)(2) = 2^2 + 1 = 4 + 1 = 5$$
$$(g \circ f)(2) = 2^2 + 2 \cdot 2 + 1 = 4 + 4 + 1 = 9$$

- **Theorem 7.3.1:**
  - Given a function $f: X \to Y$ where I_X is the identity function on X, and I_Y is the identity function on Y, then

$$f \circ I_X = f$$
$$I_Y \circ f = f$$

- **Theorem 7.3.2:**
  - If $f: X \to Y$ is a one-to-one and onto function with inverse function $f^{-1}: Y \to X$, then

$$f^{-1} \circ f = I_X$$
$$f \circ f^{-1} = I_Y$$

Composition of One-to-One Functions

- There is transitivity between compositions of one-to-one functions
- **Theorem 7.3.3:**
  - If $f: X \to Y$ and $g: Y \to Z$ are both one-to-one functions, then $g \circ f$ is one-to-one

Composition of Onto Functions

- There is transitivity between compositions of onto functions
- **Theorem 7.3.4**
  - If $f: X \to Y$ and $g: Y \to Z$ are both onto functions, then $g \circ f$ is onto

▼ [7.4] Cardinality with Applications to Computability

- A set has the same **cardinality** of another set if, and only if, there is exists a one-to-one correspondence between them
- Additionally, if two finite sets' elements can be be paired by a one-to-one correspondence, then they have the same size
- **Theorem 7.4.1:** Properties of cardinality
  - For all sets A, B, and C
    - **Reflexive property:** A has the same cardinality as A

    - **Symmetric property:** If A has the same cardinality as B, then B has the same cardinality of A
    - **Transitive property:** if A has the same cardinality as B, and B has the same cardinality as C, then A has the same cardinality of C
    - I am NOT proving ts, like if a corresponds to b, and b corresponds to c, then a corresponds to c? like, no shi

- For instance, an infinite set and its proper subset may have the same cardinality
  - The set of all even integers, $2\mathbb{Z}$ has the same cardinality as $\mathbb{Z}$
  - Suppose $H: \mathbb{Z} \to 2\mathbb{Z}$ is defined as follows

$$H(n) = 2n \quad \text{for each } n \in \mathbb{Z}$$

  - *Show that H is one-to-one*
  - Suppose there are some integers n_1 and n_2 such that

$$H(n_1) = H(n_2)$$

  - Thus,

$$\begin{aligned} 2n_1 &= 2n_2 \\ n_1 &= n_2 \end{aligned}$$

  - *Show that H is onto*
  - Suppose m is any element of $2\mathbb{Z}$
  - By definition of even, $m = 2k$ for some integer k
  - Thus, by substitution, $H(k) = 2k = m$
  - Because there exists a $k \in \mathbb{Z}$ for $H(k) = m$, H is onto
  - Thus, H is a one-to-one correspondence and $\mathbb{Z}$ and $2\mathbb{Z}$ must have the same cardinality

Countable Sets

- The most basic infinite sets is $\mathbb{Z}^+$, the set of counting numbers

$$\begin{pmatrix} \mathbb{Z}^+ \\ 1 \\ 2 \\ 3 \\ \dots \\ \dots \end{pmatrix} \begin{matrix} \xrightarrow{F} \\ \to \\ \to \\ \to \\ \to \\ \to \end{matrix} \begin{pmatrix} A \\ \text{First element of } A \\ \text{Second element of } A \\ \text{Third element of } A \\ \dots \\ \dots \end{pmatrix}$$

- A set is **countably infinite** if, and only if, it has the same cardinality as $\mathbb{Z}^+$
- A set is **countable** if, and only if, it is finite or countably infinite
    - Otherwise, the set is **uncountable**
- Ex: *Show that $\mathbb{Z}$ is countable*
    - *Since $\mathbb{Z}$ is not finite, to prove that it is countable it must be shown that it is countably infinite. Therefore, a function with a one-to-one correspondence between from $\mathbb{Z}$ to $\mathbb{Z}^+$ is needed*
    - A way to think about this problem is how $\mathbb{Z}$ may be counted (using elements of $\mathbb{Z}^+$)
    - Since the set of all integers goes in two directions, counting can be done by alternating between positive integers and negative integers

$$\begin{array}{llccccccccl} \text{Integers:} & \dots & -3 & -2 & -1 & 0 & 1 & 2 & 3 & \dots \\ \text{Count:} & & 7 & 5 & 3 & 1 & 2 & 4 & 6 & \end{array}$$

$$\therefore 0, 1, -1, 2, -2, 3, -3, \dots$$

    - Notice how every odd count represents a negative number while every even count represents a positive number
    - Thus, thinking of a count of n, the following rule may be derived

$$F(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is an even positive integer} \\ -\frac{n-1}{2} & \text{if } n \text{ is an odd positive integer} \end{cases}$$

The Search for Larger Infinites: The Cantor Diagonalization Process

- Prove that $\mathbb{Q}^+$ is countable
    - The elements of $\mathbb{Q}^+$ may be expressed using a grid organized by increasing numerators and denominators
    - *To show that $\mathbb{Q}^+$ and $\mathbb{Z}^+$ have the same cardinality, a counting method is needed to traverse the grid*

1. Traverse right once
2. Traverse diagonally to the bottom left until the leftmost column is reached (denominator equals 1)
3. Traverse downward once
4. Traverse diagonally to the top right until the first row is reached (numerator equals 1)
5. Repeat
    - *For all steps, ignore equivalent fractions*

$$\begin{array}{cccc}
\frac{1}{1}^{\text{1st}} & \frac{1}{2}^{\text{2nd}} & \frac{1}{3}^{\text{5th}} & \cdots \\
\frac{2}{1}^{\text{3rd}} & \cancel{\frac{2}{2}} & \frac{2}{3}^{\text{7th}} & \cdots \\
\frac{3}{1}^{\text{4th}} & \frac{3}{2}^{\text{8th}} & \cancel{\frac{3}{3}} & \cdots \\
\vdots & \vdots & \vdots & \ddots
\end{array}$$

- As a rule for $F \colon \mathbb{Z}^+ \to \mathbb{Q}^+$

$$\begin{gathered}
F(1) = 1 \\
F(2) = \frac{1}{2} \\
F(3) = 2 \\
F(4) = 3 \\
\text{Skip } \frac{2}{2} \\
F(5) = \frac{1}{3} \\
\cdots
\end{gathered}$$

  - The grid contains every positive rational number, and the counting method will reach every single element in the grid, so F is onto
  - Additionally, since equivalent fractions are skipped, no rational number is counted twice, so F is one-to-one
  - Thus, F is a one-to-one correspondence, and $\mathbb{Z}^+$ and $\mathbb{Q}^+$ have the same cardinality
  - Hence $\mathbb{Q}^+$ is countably infinite and countable

- **Theorem 7.4.2:**
  - The set of all real numbers between 0 and 1 is uncountable
- **Theorem 7.4.3**
  - The subset of any countable set is countable
- **Corollary 7.4.4**
  - Any set with an uncountable subset is uncountable

Application: Cardinality and Computability

- Show that the set of all computer programs in a given computer language is countable

- A computer program in any language can be thought of as a finite string of symbols in the finite alphabet of the language
- Thus, given any computer language, let P be the set of all computer programs in the language
- P is either finite or infinite
- **Case 1:** P is finite
    - In this case, P is finite and thus countable
- **Case 2:** P is infinite
    - Binary code may be used to translate the language's alphabet symbols into 0s and 1s
    - Order these strings by their length in ascending order
        - *Note: This is necessary because if the binary values are viewed purely numerically and ignoring leading zeros, then 0010 could be seen as equal to 00010*
    - $F: \mathbb{Z}^+ \to P$ may be defined as

$$F(n) = n\text{th program of the list for each } n \in \mathbb{Z}^+$$

    - By construction, F is one-to-one and onto
    - Thus, P is countably infinite, and—by extension—countable

- Prove that a particular set is uncountable such that there must exist an uncomputable function
    - **Part 1:** Show that T, the set of all functions from $\mathbb{Z} \to \{\, x \in \mathbb{Z} \mid 1 \leq x \leq 9 \,\}$, is uncountable
        - Let S be the set of all real numbers between 0 and 1 where each element is in the form

$$0.a_1a_2a_3 \ldots a_n \ldots,$$

        - where each a_i is an integer from 0 to 9
        - *This is unique as long as decimals ending in all 9s are not counted*
        - This can be defined as a rule from S to subset T

$$F(0.a_1a_2a_3 \ldots a_n \ldots) = \text{the function that sends each positive integer } n \text{ to } a_n$$

        - F is onto because T is a subset of S

    - F is one-to-one because $F(x_1)$ and $F(x_2)$ are only equal if they have the same decimal digit for each positive integer, implying $x_1 = x_2$
    - Thus, F is a one-to-one correspondence from S to subset T
    - However, S is uncountable according to Theorem 7.4.2
    - Thus, by Corollary 7.4.4, T is also uncountable
- **Part 2:** Derive a consequence of there being uncomputable functions
    - The previous part shows that T is uncountable
    - But, according to the previous example, the set of all computer programs in a programming language is countable
    - Consequently, there are not enough programs to compute the values of every function in T, meaning that there must exist functions that aren't computable