FUNCTIONS AND RELATIONS

FRANK TSAI

Contents

1. Relations

Definition 1.1. An n-ary *relation* R on a set S can be encoded as a subset:

$$R \subseteq S^n$$

We write $R(a, \dots, z)$ whenever $(a, \dots, z) \in R$. Binary relations will be the main focus of this class. For these relations, it is customary to use infix notations. That is, we write aRb instead of $R(a, b)$.

Example 1.2. The substring relation $\sqsubseteq$ on $\{a, b\}^*$ is the subset

$$\{(\varepsilon, \varepsilon), (\varepsilon, a), \dots, (a, a), (a, ab), (a, ba), \dots\}$$

Example 1.3. The divisibility relation $\mid$ on $\mathbb{Z}$ is defined by

$$a \mid b \iff \exists c.\, b = ac$$

It is the subset

$$\{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \exists c.\, b = ac\}$$

Example 1.4. The adjacency relation on a simple graph: two vertices u are v are adjacent if they are connected by an edge. It is the subset

$$\{(u, v) \in V \times V \mid (u, v) \in E \vee (v, u) \in E\}$$

Definition 1.5 (Reflexivity). A binary relation R on a set S is *reflexive* if every element of S is related to itself by R.

$$\forall a.\, aRa$$

Example 1.6. The divisibility relation on $\mathbb{Z}$ is reflexive because every integer divides into itself once.

Definition 1.7 (Symmetry). A binary relation R on a set S is *symmetric* if whenever a is related to b by R, then b is also related to a by R.

$$\forall a. \forall b.\, (aRb \Rightarrow bRa)$$

Example 1.8. The adjacency relation on a simple graph is symmetric. If a vertex u is adjacent to another vertex v, then v is also adjacent to u.

Definition 1.9 (Transitivity)**.** A binary relation R on a set S is *transitive* if for any three elements a, b, c of S, if aRb and bRc then aRc.

$$\forall a. \forall b. \forall c. \, (aRb \wedge bRc \Rightarrow aRc)$$

Example 1.10. The substring relation on $\{a, b\}^*$ is transitive. In fact, it is also reflexive, but it is not symmetric.

Definition 1.11 (Equivalence Relation)**.** A binary relation R on a set S is an *equivalence relation* if it is

  (i) reflexive,
 (ii) symmetric, and
(iii) transitive.

Proposition 1.12. *The congruence-modulo-2 relation on $\mathbb{Z}$ is defined by*

$$a \equiv b \mod 2 \iff 2 \mid (a - b)$$

It is an equivalence relation.

Proof. (Reflexivity). Let a be any integer. We need to prove that $a \equiv a \mod 2$. By definition, this is equivalent to proving $2 \mid (a - a)$, or equivalently, $2 \mid 0$. By definition again, this is equivalent to $\exists c. \, 0 = 2c$. Setting $c := 0$ yields $0 = 2 \cdot 0 = 0$ as desired.

    (Symmetry). Let a, b be any integers. Assume that $a \equiv b \mod 2$. By definition, this hypothesis asserts that there's an integer c so that $a - b = 2c$. We need to prove $\exists k. \, b - a = 2k$. Setting $k := -c$ yields $b - a = -(a - b) = -2c = 2(-c)$ as desired.

    (Transitivity). Let a, b, c be any integers. Assume that $a \equiv b \mod 2$ and that $b \equiv c \mod 2$. By definition, these two hypotheses assert that there are integers n, m so that $a - b = 2n$ and $b - c = 2m$. We need to show that $\exists k. \, a - c = 2k$. Setting $k := n + m$ yields $2(n + m) = 2n + 2m = (a - b) + (b - c) = a - b + b - c = a - c$ as desired. $\qquad\square$

Definition 1.13 (Antisymmetry)**.** A binary relation R on a set S is *antisymmetric* if for any two elements a, b of S, if aRb and bRa then $a = b$.

Example 1.14. The subset relation $\subseteq$ on $\mathcal{P}(S)$ is antisymmetric. Recall that two sets A and B are equal precisely when $A \subseteq B$ and $B \subseteq A$.

Remark 1.15. Antisymmetry does **not** imply **a**symmetry. For example, the indiscrete relation I on the singleton set $\{a\}$, defined as

$$I = \{(a, a)\}$$

is both antisymmetric and symmetric.

Definition 1.16 (Preorder)**.** A binary relation is a *preorder* if it is

 (i) reflexive, and
(ii) transitive.

Definition 1.17 (Partial Order)**.** A *partial order* is a preorder that additionally satisfies antisymmetry.

Proposition 1.18. *The divisibility relation on $\mathbb{N}$ is a partial order.*

Proof. (Reflexivity): Exercise.

(Transitivity): Exercise. Hint: See Proposition 1.12.

(Antisymmetry): Let a, b be natural numbers so that $a \mid b$ and $b \mid a$. These hypotheses assert that there are natural numbers n, m so that $b = an$ and that $a = bm$. Thus, $b = (bm)n$. If $b = 0$, then since $a = bm = 0m = 0$, $a = b$ as desired. However, if $b \neq 0$, then $mn = 1$. Since n, m are natural numbers, $n = m = 1$. Thus, $a = b$ as desired. □

Remark 1.19. Proposition 1.18 does not hold if we replace $\mathbb{N}$ with $\mathbb{Z}$ because $2 \mid -2$ and $-2 \mid 2$, but $2 \neq -2$. Although the divisibility relation on $\mathbb{Z}$ is not a partial order, it is a preorder.

2. FUNCTIONS

Intuitively, a function is a rule for assigning each element of a set to a unique element of another set. In set theory, functions can be encoded as a special binary relation.

Definition 2.1. A binary relation $R \subseteq A \times B$ is (left) *total* if

$$\forall a \in A. \exists b \in B. (a, b) \in R$$

Definition 2.2. A binary relation $R \subseteq A \times B$ is *functional* if

$$\forall a \in A. \forall b \in B. \forall c \in C. ((a, b) \in R \wedge (a, c) \in R \Rightarrow b = c)$$

Definition 2.3. A function f from a set A to another set B, denoted $f : A \to B$ is a binary relation

$$f \subseteq A \times B$$

such that f is *total* and *functional*. We write $f(a) = b$ for $(a, b) \in f$. Writing the two conditions in this notation is perhaps more illuminating:

(i) Totality:

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

(ii) Functionality:

$$\forall a \in A. \forall b \in B. \forall c \in C. (f(a) = b \wedge f(a) = c \Rightarrow b = c)$$

The set A is called the *domain* of f, and the set B is called the *codomain* of f.

Theorem 2.4 (Functional Extensionality). *Two functions $f, g : A \to B$ are equal if and only if $f(a) = g(a)$ for all $a \in A$.*

Proof. The "only if" direction is obvious. For the "if" direction, assume that $f(a) = g(a)$ for all $a \in A$. To prove that $f = g$, it suffices to prove $f \subseteq g$ and $g \subseteq f$. Now, suppose that $(a, b) \in f$. Since $f(a) = g(a)$, $(a, g(a)) \in f$. By functionality, $g(a) = b$. Thus, $(a, b) \in g$, proving that $f \subseteq g$. The proof of $g \subseteq f$ is completely analogous. □

Definition 2.5. Given two functions $f : A \to B$ and $g : B \to C$, the composition $g \circ f : A \to C$ (reads "g after f") is a function defined by

$$(g \circ f)(x) = g(f(x))$$

Note that $g \circ f$ is defined only if the codomain of f and the domain of g are the same.

Lemma 2.6. *Composition is associative, i.e., $(f \circ g) \circ h = f \circ (g \circ h)$.*

Proof. Exercise. Hint: Use functional extensionality. □

Definition 2.7. For any set S, there is a special function id_S, called the *identity function on S*, defined by

$$\mathrm{id}_S(s) = s$$

Lemma 2.8. *For any function $f : A \to B$, $\mathrm{id}_B \circ f = f$ and $f \circ \mathrm{id}_A = f$.*

Proof. Exercise. □

Lemmas 2.6 and 2.8 mean that sets and functions between them assemble into a category. Category theory is an interesting subject that we will sadly not discuss in this class.

Definition 2.9. A function $f : A \to B$ is *injective*, denoted $f : A \rightarrowtail B$, if

$$\forall a \in A. \forall a' \in A. \, (f(a) = f(a') \Rightarrow a = a')$$

Definition 2.10. A function $f : A \to B$ is *surjective*, denoted $f : A \twoheadrightarrow B$, if

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

Theorem 2.11 (Cantor's Theorem)**.** *For any set S, there is no surjective functions $f : S \twoheadrightarrow \mathcal{P}(S)$.*

Proof. Suppose that $f : S \twoheadrightarrow \mathcal{P}(S)$. Consider the subset $\{s \in S \mid s \notin f(s)\}$. Since f is surjective, there must be some $s' \in S$ so that $f(s') = \{s \in S \mid s \notin f(s)\}$. If $s' \in f(s')$, then by definition, $s' \notin f(s')$. Similarly, if $s' \notin f(s')$, then by definition, $s' \in f(s')$. This is a contradiction. □

Definition 2.12. A function $f : A \to B$ is *bijective* if it is injective and surjective.

Definition 2.13. A function $f : A \to B$ is *invertible* if there is a function $g : B \to A$ such that

(i) $f \circ g = \mathrm{id}_B$, and
(ii) $g \circ f = \mathrm{id}_A$.

g is called the inverse of f. When f is invertible, we write f^{-1} for its inverse.

Theorem 2.14. *A function $f : A \to B$ is invertible if and only if f is bijective.*

Proof. The "if" direction: assume that f is invertible. Then there is a function $f^{-1} : B \to A$ such that $f \circ f^{-1} = \mathrm{id}_B$ and $f^{-1} \circ f = \mathrm{id}_A$.

(Injectivity): Let $a, a' \in A$ be given. Assume that $f(a) = f(a')$. Then $\mathrm{id}_A(a) = f^{-1}(f(a)) = f^{-1}(f(a')) = \mathrm{id}_A(a')$. Thus, $a = a'$.

(Surjectivity): Let $b \in B$ be given. We need to show that there is some $a \in A$ so that $f(a) = b$. Choose $a := f^{-1}(b)$, then $f(f^{-1}(b)) = \mathrm{id}_B(b) = b$.

The "only if" direction: assume that f is bijective. We need to show that f is invertible. To this end, we construct a function $f^{-1} : B \to A$. For each $a \in A$ so that $f(a) = b$, we take $f^{-1}(b) = a$. To show that f^{-1} is a function, we must show that it is total and functional. Totality follows from surjectivity of f and functionality follows from injectivity of f. The details are left to the reader as an exercise. □

3. Countable Sets and Uncountable Sets

Definition 3.1. A set S is *countable* if there is a bijection $f : S \to \mathbb{N}$.

Theorem 3.2. $\mathbb{N}^{\mathbb{N}}$ *is uncountable.*

Proof. Suppose that $\mathbb{N}^{\mathbb{N}}$ is countable, i.e., $\mathbb{N} \cong \mathbb{N}^{\mathbb{N}}$. A possible interpretation of this hypothesis is that every function $f : \mathbb{N} \to \mathbb{N}$ can be given a unique natural-number code. That is, there are functions

$$\text{decode} : \mathbb{N} \to \mathbb{N}^{\mathbb{N}} \tag{3.3}$$

$$\text{encode} : \mathbb{N}^{\mathbb{N}} \to \mathbb{N} \tag{3.4}$$

that are mutual inverses. Consider the function

$$k : \mathbb{N} \to \mathbb{N} \tag{3.5}$$

$$k : n \mapsto \text{decode}(n)(n) + 1 \tag{3.6}$$

Given a code n, the function k decodes n, yielding a function $\mathbb{N} \to \mathbb{N}$, then evaluates that function at n, and finally adds 1 to the result.

The function k has a unique code given by $\text{encode}(k)$. Now, let's evaluate k at its own code:

$$k(\text{encode}(k)) = \text{decode}(\text{encode}(k))(\text{encode}(k)) + 1 \tag{3.7}$$

$$= k(\text{encode}(k)) + 1 \tag{3.8}$$

This is a contradiction. $\qquad\square$

Theorem 3.2 tells us that some functions $f : \mathbb{N} \to \mathbb{N}$ are uncomputable: there are only countably many programs that one can write, but there are uncountably many endofunctions on $\mathbb{N}$. Thus, some of those functions do not have a corresponding program that computes it.