Equivalence Relations

A relation that is reflexive, transitive, and symmetric is called an *equivalence relation*.

For example, the set $\{(a,a),(b,b),(c,c)\}$ is an equivalence relation on $\{a,b,c\}$.

An equivalence relation R defines "clusters" of elements of A. More formally, we define for each element $a \in A$ a set,

$$[a]_R = \{b \in A \ : \ aRb\},$$

that is also called the *equivalence class* of a (with respect to R).

If the relation R is clear from the context, we usually write $[a]$ instead of $[a]_R$.

A *partition* of a set A is a subset Π of $\mathcal{P}(A)$ such that (i) $\emptyset$ is not an element of Π and (ii) each element of A is in one, and only one, set in Π.

For example, $\{\{a\},\{b\},\{c\}\}$ and $\{\{a,c\},\{b\}\}$ are partitions of $\{a,b,c\}$, but $\{\{a\},\{b\},\{b,c\}\}$ is not.

Partitions and Equivalence Relations

Theorem.

> If R is an equivalence relation on a non-empty set A, then the equivalence classes of R constitute a partition of A.

Conversely, if Π is a partition of A, then the relation

$$\{(a,b) \ : \ a \text{ and } b \text{ are elements of the same set in } \Pi\}$$

is an equivalence relation.

In other words, there is a one-to-one correspondence between equivalence relations on A and partitions on A.

For example, the relation $\sim$ on $\mathbf{N}$, defined by

$$m \sim n \Leftrightarrow m+n \text{ is even},$$

is an equivalence that partitions the set of natural numbers into two subsets—the sets of even and odd natural numbers, respectively.

Congruence Modulo p

We define binary relations on the integers, for all integers p greater than 1, as follows.

We say that m is *congruent to n modulo p*, and write $m \equiv n (\text{mod } p)$, if $m-n$ is an integer multiple of p.

For example, take $p = 3$. Then 1 is congruent to 4 modulo p, but not congruent to 3.

Let R_p be the set

$$\{(m,n) \ : \ m \equiv n (\text{mod } p)\}.$$

> Is the relation R_p reflexive?
>
> Is it transitive?
>
> Is it symmetric?

The answer to each question is affirmative, and hence each relation R_p is an equivalence relation on the integers.

An Equivalence Relation on Strings

Let Σ be an alphabet. We define a binary relation $\sim$ on the set of strings Σ^* as follows:

$$v \sim w \text{ if and only if } |v| = |w|.$$

The relation $\sim$ is an equivalence.

Reflexivity. We have $|w| = |w|$, and hence $w \sim w$, for all strings w.

Symmetry. If $v \sim w$, then by definition $|v| = |w|$. By the symmetry of equality we thus have $|w| = |v|$, and hence $w \sim v$.

Transitivity. Suppose $u \sim v$ and $v \sim w$. Then $|u| = |v|$ and $|v| = |w|$ and therefore, by the transitivity of equality, $|u| = |w|$, which implies $u \sim w$.

Let Σ^k be the set of all strings of size k over Σ.

The collection of all sets Σ^k, $k \in \mathbf{N}$, is a partition of Σ^*. In fact, the sets Σ^k are the equivalence classes induced by $\sim$.

Equinumerous Sets

Two sets A and B are said to be *equinumerous* (or of the same size) if, and only if, there is a bijection from A to B. (Recall that a function is a bijection if it is one-to-one and onto.)

We write $A \sim B$ if A and B are of the same size in this sense. The relation $\sim$ is also an equivalence.

Reflexivity. The identity function on A is a bijection from A to A, thus $A \sim A$.

Symmetry. If there is a bijection f from A to B, then the inverse function f^{-1} is a bijection from B to A. Thus, $A \sim B$ implies $B \sim A$.

Transitivity. Suppose $A \sim B$ and $B \sim C$. Then there are bijections f from A to B and g from B to C. The composition of the two functions f and g is a bijection from A to C and thus $A \sim C$.

Finite and Infinite Sets

We call a set *finite* if it is equinumerous with some set $\{0, 1, \ldots, n-1\}$, for some natural number n.

If A is equinumerous with $\{0, 1, \ldots, n-1\}$, then it is said to be of *cardinality* n, written $|A| = n$.

If a set is not finite, it is called *infinite*.

Examples of infinite sets are the sets of natural numbers, of integers, of rational numbers, of real numbers. But not all of these sets are equinumerous, as we shall see!

A set is called *countably infinite* if it is equinumerous with the set $\mathbf{P}$ of positive natural numbers.

The set of natural numbers is countably infinite as the function f, defined by $f(n) = n + 1$, is a bijection from $\mathbf{N}$ to $\mathbf{P}$.

A set is called *countable* if it is finite or countably infinite; and *uncountable* otherwise.

Informally, one can list the elements of a countable set, though the list may never end.

The Pigeonhole Principle

The following observation is known as the *Pigeonhole Principle*:

> *If A and B are finite sets and B has fewer elements than A, then there is no one-to-one function from A to B.*

For example, how many of the integers from the set $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ need to be selected so that, regardless of the choice of selection, there is at least one pair with a sum of 9?

Four is not enough, as we may select $1, 2, 3, 4$ where no pair yields a sum larger than 7.

But any selection of five integers from A must contain a pair whose sum is 9. To see why, observe that A can be partitioned into four different subsets $A_1 = \{1, 8\}$, $A_2 = \{2, 7\}$, $A_3 = \{3, 6\}$, and $A_4 = \{4, 5\}$, where the sum of each of the four corresponding pairs is 9.

Now if a_1, a_2, a_3, a_4, and a_5 are the selected integers from A, we define a function f, by setting $f(a_i)$ to be the set A_j that contains a_i.

By the pigeonhole principle, the function f is not one-to-one, so that there exist two integers a_i and a_j with $f(a_i) = f(a_j)$. In other words, there must be one subset A_k, both of whose elements are selected. The corresponding sum is 9.

Subsets of Countable Sets

A function $f : A \to B$ is called a *one-to-one correspondence* (between A and B) if it is one-to-one and onto.

Theorem.

> Every subset of a countable set is countable.

Proof. It is sufficient to show that subsets of $\mathbf{P}$ are countable. Let A be a subset of $\mathbf{P}$.

If A is finite it is countable by definition.

Suppose A is infinite. We define a one-to-one correspondence f from $\mathbf{P}$ to A by recursion:

1. Let $f(1)$ be the smallest element of A.
2. If $n > 1$, then $f(n)$ is defined to be the smallest element of $A \setminus \{f(1), \ldots, f(n-1)\}$.

It can easily be verified that f is one-to-one and onto. ∎

The above proof uses the so-called *well-ordering principle* of the natural numbers:

> *Every non-empty subset of $\mathbf{N}$ has a smallest element.*

Cartesian Products of Countable Sets

Theorem.

> The set $\mathbf{P} \times \mathbf{P}$ is countable.

Sketch of proof. We define a one-to-one correspondence between $\mathbf{P}$ and $\mathbf{P} \times \mathbf{P}$ by "enumerating" all ordered pairs of positive natural numbers as follows.

Begin with the pair $(1,1)$, then list all pairs the components of which add up to 3, then all pairs of components that add up to 4, and so on.

$$\begin{array}{cccc} (1,1) & (1,2) & (1,3) & (1,4) & \ldots \\ (2,1) & (2,2) & (2,3) & (2,4) & \ldots \\ (3,1) & (3,2) & (3,3) & (3,4) & \ldots \\ (4,1) & (4,2) & (4,3) & (4,4) & \ldots \\ \vdots & \vdots & \vdots & \vdots & \end{array}$$

∎

Corollary

> The Cartesian product of two countable sets is countable.

Proof. Let A and B be countable sets. Thus there are one-to-one correspondences f between A and $\mathbf{P}$ and g between B and $\mathbf{P}$. But then the function h defined by $h(x,y) = (f(x), g(y))$ is a one-to-one correspondence between $A \times B$ and $\mathbf{P} \times \mathbf{P}$.

It follows immediately from the definition of countability that if there is a one-to-one correspondence between two sets X and Y, then one set is countable if and only if the other is countable.

We already know that $\mathbf{P} \times \mathbf{P}$ is countable. Consequently $A \times B$ is also countable. ∎

Examples of Countable Sets

The set of integers $\mathbf{Z}$ is countable. A suitable bijection from $\mathbf{Z}$ to $\mathbf{P}$ is the function f, defined by:

$$f(n) = \begin{cases} 2n+1 & \text{if } n \geq 0 \\ -2n & \text{if } n < 0 \end{cases}$$

Surprisingly, the set of rational numbers $\mathbf{Q}$ is also countable.

Proof. The set of integers $\mathbf{Z}$ is countable. Hence by the above theorem, the set $\mathbf{Z} \times \mathbf{Z}$ is also countable.

But the set of rational numbers $\mathbf{Q}$ is a subset of $\mathbf{Z} \times \mathbf{Z}$, and therefore is also countable. ∎

Countability of Formal Languages

Theorem.

> The set Σ^* of all strings over an alphabet Σ is countable.

Proof. We use the fact that

$$\Sigma^* = \bigcup_{k \in \mathbf{N}} \Sigma^k,$$

where Σ^k denotes the set of all strings of length k.

Since all sets Σ^k are countable, there are corresponding *one-to-one* functions $f_k : \Sigma^k \to \mathbf{N}$.

We define a function $f : \Sigma^* \to \mathbf{N} \times \mathbf{N}$ by:

$$f(w) = (f_{|w|}(w), |w|).$$

The function f is one-to-one. (If $f(w) = f(v)$, then $|w| = |v|$ and $f_{|w|}(w) = f_{|v|}(v) = f_{|w|}(v)$. But since $f_{|w|}$ is one-to-one, we may conclude that $w = v$.)

By the theorems we proved previously, Σ^* is countable.

∎

Note that the proof does not depend on the assumption that Σ is finite, but shows that the statement is valid for infinite sets Σ as well.

The Diagonalization Principle

We next discuss a mathematical proof technique that has important applications in the theory of computation.

The Diagonalization Principle.

> Let R be a binary relation on a set A, and let D, the *diagonal set* for R, be $\{a \in A \ : \ (a,a) \in R\}$. We denote by $\bar{D}$ the complement, $A \setminus D$, of D and, for each $x \in A$, by R_x the set $\{y \in A \ : \ (x,y) \in R\}$.
>
> The set $\bar{D}$ is distinct from each set R_a.

We illustrate this principle by an example.

Example of Diagonalization

For example, let R be the binary relation

$$\{(a,b),(a,d),(b,b),(b,c),(c,c),(d,b),(d,c),(d,e),(e,e)\}.$$

This relation can be represented by a table:

	a	b	c	d	e
a		x		x	
b		x	x		
c			x		
d		x	x		x
e					x

We have

$$\begin{aligned} R_a &= \{b,d\} \\ R_b &= \{b,c\} \\ R_c &= \{c\} \\ R_d &= \{b,c,e\} \\ R_e &= \{e\} \end{aligned}$$

and $\bar{D} = \{a,d\}$.

Note that these sets correspond to the rows in the above table. The set $\bar{D}$ is represented by a sequence of boxes

x			x	

that is different from each row in the above table.

Application of Diagonalization: Uncountable Sets

Theorem.

> The powerset of $\mathbf{N}$ is uncountable.

Proof. We prove the theorem by contradiction. Suppose $\mathcal{P}(\mathbf{N})$ is countable. Then there is a one-to-one correspondence f between $\mathbf{N}$ and $\mathcal{P}(\mathbf{N})$.

We first define a binary relation

$$R = \{(i,j) \in \mathbf{N} \times \mathbf{N} \ : \ j \in f(i)\}.$$

The set R_i, as defined in the statement of the diagonalization principle, is equal to the set $f(i)$. In other words, each subset of $\mathbf{N}$ is equal to one of the sets R_i.

Now consider the diagonal set for R,

$$D = \{n \in \mathbf{N} \ : \ n \in R_n\}.$$

By the diagonalization principle, the set $\bar{D}$ is distinct from each set R_i.

But $\bar{D}$ is a subset of $\mathbf{N}$, and since f is a one-to-one correspondence between $\mathbf{N}$ and $\mathcal{P}(\mathbf{N})$, we must have $\bar{D} = R_k$ for some k.

In short, the assumption that $\mathcal{P}(\mathbf{N})$ is countable leads to a contradiction. Thus we have proved that $\mathcal{P}(\mathbf{N})$ is not countable. ∎