MAT 258
Discrete Mathematics
Basic Structures

Kenneth H. Rosen and Kamala Krithivasan

Discrete Mathematics 7E Global Edition Chapter 2

Fall 2018 Weeks 1–2

Sets by Roster Method

A **set** is an unordered collection of objects, called **elements** or **members** of the set. A set is said to **contain** its elements. We write $a \in A$ to denote that a is an element of the set A. The notation $a \notin A$ denotes that a is not an element of the set A. Listing the elements of a set is describing the set by the **roster method**.

- The set V of all vowels in the English alphabet: $V = \{\text{`a`}, \text{`e`}, \text{`i`}, \text{`o`}, \text{`u`}\}$
- The set O of odd positive integers less than 10: $O = \{1, 3, 5, 7, 9\}$

Nothing prevents a set from having seemingly unrelated elements: consider the set $\{a, 2, \texttt{Fred}, \texttt{New Jersey}\}$.

The roster method need not list all the members: some members are listed, then **ellipses** $(\dots)$ are used when the general pattern is obvious. The set of positive integers less than 100 can be denoted by $\{1, 2, 3, \dots, 99\}$.

Set Builder Notation

Another way to describe a set is to use **set builder** notation. We characterize all those elements in the set by stating the property or properties they must have to be members. The set O of positive integers less than 10:
$O = \{x \mid x \text{ is an odd positive integer less than } 10\} = \{x \in \mathbb{Z}^+ \mid x \text{ is odd and } x < 10\}$.
This is often used when it is impossible to list all the elements of the set.

- $\mathbb{N} = \{1, 2, 3, \ldots\}$, the set of **natural numbers** (what the book refers to as $\mathbb{Z}^+$, the set of **positive integers**—what the book calls natural: $\{0, 1, 2, 3, \ldots\} = \mathbb{W}$, the set of **whole numbers**)
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, the set of **integers**
- $\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z}, q \neq 0\}$, the set of **rational numbers**
- $\mathbb{R}$, the set of **real numbers**, $\mathbb{R}^+$, the set of **positive reals**
- $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i = \sqrt{-1}\}$, the set of **complex**

More Examples

Intervals of real numbers: when $a, b \in \mathbb{R}$ with $a < b$

- $[a, b] = \{x \mid a \leq x \leq b\}$, the **closed interval**
- $[a, b) = \{x \mid a \leq x < b\}$
- $(a, b] = \{x \mid a < x \leq b\}$
- $(a, b) = \{x \mid a < x < b\}$, the **open interval**

The set $\{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$ is a set containing four elements, each of which is a set.

A **datatype** or **type** is the name of a set, together with a set of operations that can be performed on objects from that set. For example, *boolean* is the name of the set $\{0, 1\}$ with operators on one or more elements if this set, such as `AND`, `OR` and `NOT`.

Equality of Sets, Some Special Sets

Two sets are **equal** if and only if they have the same elements: for sets A and B, the sets are equal ($A = B$) if and only if $\forall x(x \in A \leftrightarrow x \in B)$—that is, for all objects x, x is an element of A if and only if x is an element of B.

The sets $\{1, 3, 5\}$ and $\{3, 5, 1\}$ are equal—note that the order in which the elements of a set are listed does not matter. Also, it does not matter if an element of a set is listed more than once: $\{1, 3, 3, 3, 5, 5, 5, 5\}$ is the same as the set $\{1, 3, 5\}$.

The **empty set** or **null set**, denoted by $\emptyset$, is the special set that has no elements. It is also denoted as $\{\}$. Often, a set of elements with certain properties turns out to be the null set: for instance, the set of all positive integers greater than their squares.

A set with one element is called a **singleton set**. Note that the empty set $\emptyset$ is not equal to the singleton set $\{\emptyset\}$.

Naive Set Theory

The term **object** has been used in the definition of a set without specifying what an object is. This description of a set as a collection of objects, **based on the intuitive notion of an object**, was first stated in 1895 by Georg Cantor. The theory that results from this intuitive definition of a set, and the use of intuitive notion that **for any property whatever, there is a set consisting of exactly the objects with this property**, leads to **paradoxes**, or logical inconsistencies. This was shown by the English philosopher Bertrand Russell in 1902. These logical inconsistencies can be avoided by building set theory beginning with axioms (axiomatic set theory).

However, we will use Cantor's original version of set theory, known as **naive set theory**, in this book because all sets considered can be treated consistently using Cantor's original theory.

Venn Diagram

Sets can be represented graphically using **Venn diagrams**. In Venn diagrams, the **universal set** $\mathcal{U}$, which contains all the objects under consideration, is represented by a rectangle. Inside this rectangle, circles or other geometrical figures represent sets. Sometimes, points are used to represent particular elements of a set. Venn diagrams are often used to indicate the relationships between sets.

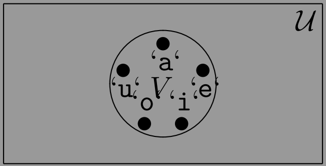

Figure: Venn Diagram for the Set of Vowels

Subsets

The set A is a **subset** of B if and only if every element of A is also an element of B, denoted as $A \subseteq B$ (or $B \supseteq A$). $A \subseteq B$ if and only if $\forall x(x \in A \to x \in B)$.

To show that $A \subseteq B$, show that if $x \in A$, then $x \in B$. O is a subset of the set of all positive integers less than 10. $\mathbb{Q} \subseteq \mathbb{R}$. The set of all computer science majors at your school is a subset of all students at your school. The set of all people in China is a subset of all people in China.

To show that $A \nsubseteq B$, determine $x \in A$ such that $x \notin B$. The set of integers with squares less than 100 is not a subset of the set of nonnegative integers, because -1 is in the former, but not the latter. The set of people who have taken discrete mathematics at your school is not a subset of the set of all computer science majors at your school if there is at least one student who has taken discrete mathematics who is not a computer science major.

Proper Subsets

For every set S, $\emptyset \subseteq S$ and $S \subseteq S$.

A is a **proper subset** of B, denoted $A \subset B$, if $A \subseteq B$, and $A \neq B$. That is: $\forall x(x \in A \rightarrow x \in B) \wedge \exists x(x \in B \wedge x \notin A)$. The Venn diagram for a set being a subset of another set is two shapes, one within the other.

If $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Sets may have other sets as members. For instance, we have the sets $A = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ and $B = \{x \mid x \text{ is a subset of } \{a, b\}\}$—note that $A = B$ and $\{a\} \in A$ but $a \notin A$.

Cardinality of Sets

If there are exactly n distinct elements in a set S, where n is a nonnegative integer, then S is a **finite set** and that n is the **cardinality** of S: $|S| = n$. A **cardinal number** is commonly used to denote the size of a finite set.
$|O| = 5$. Let S be the set of letters in the English alphabet. Then $|S| = 26$. $|\emptyset| = 0$.
A set is said to be **infinite** if it is not finite.
The set of positive integers is infinite.

Power Sets

Given a set S, the **power set** of S, $\mathcal{P}(S)$, is the set of all subsets of the set S.
$\mathcal{P}(\{0,1,2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\}$.
$\mathcal{P}(\emptyset) = \{\emptyset\}$. $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.
If a set has n elements, then its power set has 2^n elements.

Cartesian Product of Sets

The **ordered n-tuple** $(a_1, a_2, \ldots, a_n)$ is the ordered collection that has a_1 as its first element, a_2 as its second element, $\ldots$, and a_n as its nth element.

Two ordered n-tuples are equal if and only if each corresponding pair of their elements is equal—that is, $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ if and only if $a_i = b_i$ for $i = 1, 2, \ldots, n$. Ordered 2-tuples are called **ordered pairs**.

Let A and B be sets. The **Cartesian product** of A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$. Hence, $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$.

Let A represent the set of all students at a university, and let B represent the set of all courses offered at the university. $A \times B$ consists of all the ordered pairs of the form (a, b), where a is a student at the university and b is a course offered at the university.

Examples 17–20

$\{1,2\} \times \{a,b,c\} = \{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\}$.

Note that $A \times B \neq B \times A$ unless $A = \emptyset$, $B = \emptyset$ or $A = B$.

$\{a,b,c\} \times \{1,2\} = \{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\}$.

The **Cartesian product** of the sets A_1, A_2, …, A_n, denoted by $A_1 \times A_2 \times \cdots \times A_n = \prod_{i=1}^{n} A_i$, is the set of ordered n-tuples $(a_1, a_2, \ldots, a_n)$, where $a_i \in A_i$ for $i = 1, 2, \ldots, n$.In other words,

$$\prod_{i=1}^{n} A_i = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ for } i = 1, 2, \ldots, n\}.$$

$\{0,1\} \times \{1,2\} \times \{0,1,2\} = \{(0,1,0),(0,1,1),(0,1,2),(0,2,0),(0,2,1),(0,2,2),(1,1,0),(1,1,1),(1,1,2),(1,2,0),(1,2,1),(1,2,2)\}$.

Note that when A, B and C are sets, $(A \times B) \times C \neq A \times B \times C$.

$A^2 = A \times A$, $A^3 = A \times A \times A$, $A^4 = A \times A \times A \times A$—more generally, $A^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A \text{ for } i = 1, 2, \ldots, n\}$.

$A = \{1,2\}$: $A^2 = \{(1,1),(1,2),(2,1),(2,2)\}$; $A^3 = \{(1,1,1),(1,1,2),(1,2,1),(1,2,2),(2,1,1),(2,1,2),(2,2,1),(2,2,2)\}$.

Relations

A subset R of the Cartesian product $A \times B$ is called a **relation** from the set A to the set B. For example $R = \{(a, 0), (a, 1), (a, 3), (b, 1), (b, 2), (c, 0), (c, 3)\}$ is a relation from the set $\{a, b, c\}$ to the set $\{0, 1, 2, 3\}$. A relation from a set A to itself is called a relation on A.

The ordered pairs in the less than or equal to relation, which contains (a, b) if $a \leq b$, on the set $\{0, 1, 2, 3\}$ is $\{(0, 0), (0, 1), (0, 2), (0, 3), (1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$.

Relations and their properties are discussed in Chapter 9.

Set Notation with Quantifiers

Sometimes the domain of a quantified statement is explicitly restricted by making use of particular notation. For example, $\forall x(P(x))$ denotes the univeral quantification of $P(x)$ over all elements in the set S—in other words, $\forall x \in S(P(x))$ is shorthand for $\forall x(x \in S \to P(x))$. Similarly, $\exists x \in S(P(x))$ denotes the existential quantification of $P(x)$ over all elements in S—that is, $\exists x \in S(P(x))$ is shorthand for $\exists x(x \in S \land P(x))$. $\forall x \in \mathbb{R}(x^2 \geq 0)$ states that for every real number x, $x^2 \geq 0$—a true statement. $\exists x \in \mathbb{Z}(x^2 = 1)$ states that there exists an integer x such that $x^2 = 1$—a true statement.

The **truth set** of a predicate P on a domain D is the set of elements x in D for which $P(x)$ is true, denoted by $\{x \in D \mid P(x)\}$. $\{x \in \mathbb{Z} \mid |x| = 1\} = \{-1, 1\}$, $\{x \in \mathbb{Z} \mid x^2 = 2\} = \emptyset$, $\{x \in \mathbb{Z} \mid |x| = x\} = \mathbb{W}$.

Note that $\forall x P(x)$ is true over the domain U if and only if the truth set of P is the set U. Likewise, $\exists x P(x)$ is true over the

Union and Intersection of Sets

The **union** of the sets A and B, denoted by $A \cup B$, is the set that contains those elements that are either in A or in B, or in both. Thus, $A \cup B = \{x \mid x \in A \vee x \in B\}$.

$\{1, 3, 5\} \cup \{1, 2, 3\} = \{1, 2, 3, 5\}$. The union of the set of all computer science majors at your school and the set of all mathematics majors at your school is the set of students at your school who are majoring either in mathematics or in computer science (or in both).

The **intersection** of the sets A and B, denoted by $A \cap B$, is the set containing those elements in both A and B. Thus, $A \cap B = \{x \mid x \in A \wedge x \in B\}$.

$\{1, 3, 5\} \cap \{1, 2, 3\} = \{1, 3\}$. The intersection of the set of all computer science majors at your school and the set of all mathematics majors at your school is the set of students at your school who are majoring either in mathematics and in computer science.

Principle of Inclusion-Exclusion

Two sets are called **disjoint** if their intersection is the empty set. $\{1, 3, 5, 7, 9\}$ and $\{2, 4, 6, 8, 10\}$ are disjoint sets. $|A| + |B| = |A \cup B|$ only if A and B are disjoint—otherwise, $|A| + |B|$ counts $|A \cap B|$ twice. Thus, $|A \cup B| = |A| + |B| - |A \cap B|$. The generalization of this result to unions of an arbitrary number of sets is called the **principle of inclusion-exclusion**.

The principle of inclusion-exclusion is discussed along with other enumeration techniques in Chapter 8.

Difference of Sets and the Complement of a Set

The **difference** of sets A and B, denoted by $A \setminus B$ (or $A - B$), is the set containing those elements that are in A but not in B. The difference of A and B is also called the **complement of B with respect to A**. Thus, $A - B = \{x \mid x \in A \land x \notin B\}$. $\{1,3,5\} - \{1,2,3\} = \{5\}$. $\{1,2,3\} - \{1,3,5\} = \{2\}$. The difference of the set of all computer science majors at your school and the set of all mathematics majors at your school is the set of all computer science majors at your school who are not mathematics majors.

Let $\mathcal{U}$ be the universal set: the **complement** of the set A, donated by $\bar{A}$, is the complement of A with respect to $\mathcal{U}$. Therefore, the complement of the set A is $\mathcal{U} - A$. Thus, $\bar{A} = \{x \in \mathcal{U} \mid x \notin A\}$.

If $\mathcal{U}$ is the set of the letters of the English alphabet, and V is the set of vowels, then $\bar{V} = \{\text{`b'}, \text{`c'}, \text{`d'}, \text{`f'}, \text{`g'}, \text{`h'}, \text{`j'}, \text{`k'}, \text{`l'}, \text{`m'}, \text{`n'}, \text{`p'}, \text{`q'}, \text{`r'}, \text{`s'}, \text{`t'}, \text{`v'}, \text{`w'}, \text{`x'}, \text{`y'},$

Set Identities

Name of law	Identity	
Identity	$A \cap \mathcal{U} = A$	$A \cup \emptyset = A$
Domination	$A \cup \mathcal{U} = \mathcal{U}$	$A \cap \emptyset = \emptyset$
Idempotent	$A \cup A = A$	$A \cap A = A$
Complementation	$\overline{(\bar{A})} = A$	
Commutative	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associative	$A \cup (B \cup C) = (A \cup B) \cup C$	
	$A \cap (B \cap C) = (A \cap B) \cap C$	
Distibutive	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	
	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	
De Morgan's	$\overline{A \cap B} = \bar{A} \cup \bar{B}$	$\overline{A \cup B} = \bar{A} \cap \bar{B}$
Absorption	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Complement	$A \cup \bar{A} = \mathcal{U}$	$A \cap \bar{A} = \emptyset$

Table: Set Identities

Proving

Methods to prove a set identity:

- Show that the two sets being equated in the identity is each the subset of the other: $\overline{A \cap B} = \bar{A} \cup \bar{B}$ in Example 10; $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ in Example 12
- Use set builder notation and logical equivalences: $\overline{A \cap B} = \bar{A} \cup \bar{B}$ in Example 11
- Use a **membership table**: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ in Example 13
- Use established set identities: $\overline{A \cup (B \cap C)} = (\bar{C} \cup \bar{B}) \cap \bar{A}$ in Example 14

Generalized Unions and Intersections

$\{0,2,4,6,8\} \cup \{0,1,2,3,4\} \cup \{0,3,6,9\} = \{0,1,2,3,4,6,8,9\}$
$\{0,2,4,6,8\} \cap \{0,1,2,3,4\} \cap \{0,3,6,9\} = \{0\}$

The **union** of a collection of sets is the set that contains those elements that are members of at least one set in the collection, denoted by $A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$ for the n sets $A_1, \ldots, A_n$.

The **intersection** of a collection of sets is the set that contains those elements that are members of all the sets in the collection, denoted by $A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$ for the n sets $A_1, \ldots, A_n$.

For $i = 1, 2, \ldots$, let $A_i = \{i, i+1, \ldots\}$. Then, $\bigcup_{i=1}^{n} A_i = A_1$and $\bigcap_{i=1}^{n} A_i = A_n$.

Unions and Intersections of Collections

For $\{A_i\}_{i=1}^{\infty}$, $\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup \cdots \cup A_n \cup \cdots$ and $\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap \cdots \cap A_n \cap \cdots$. More generally, when I is (an index) set, $\bigcup_{i \in I} A_i = \{x \mid \exists i \in I(x \in A_i)\}$ denotes the union of the sets A_i, $i \in I$, and $\bigcap_{i \in I} A_i = \{x \mid \forall i \in I(x \in A_i)\}$ denotes the intersection of the sets A_i.

Suppose that $A_i = \{1, 2, 3, \ldots, i\}$ for $i = 1, 2, 3, \ldots$. Then, $\bigcup_{i=1}^{\infty} A_i = \mathbb{N}$ and $\bigcap_{i=1}^{\infty} A_i = \{1\}$.

Computer Representations of Sets

Assume that the universal set $\mathcal{U}$ is finite (and of reasonable size). Specify an arbitrary order of the elements of $\mathcal{U}$, $a_1, a_2, \ldots, a_n$. Represent a subset A of $\mathcal{U}$ with the bit string of length n, where the ith bit in this string is 1 if $a_i \in A$ and is 0 if $a_i \notin A$.

Let $\mathcal{U} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, with $a_i = i$, $i = 1, \ldots, 10$. The odd integers of $\mathcal{U}$ is represented by 1010101010. The even integers of $\mathcal{U}$ is represented by 0101010101. The integers not exceeding 5 in $\mathcal{U}$ is represented by 1111100000.

The complement of the set of odd integers of $\mathcal{U}$ is represented by 0101010101, switching 0s and 1s in 1010101010. The union of the set of integers not exceeding 5 in $\mathcal{U}$ and the set of odd integers of $\mathcal{U}$ is represented by 1111101010 $= 1111100000 \vee 1010101010$. The intersection of the set of integers not exceeding 5 in $\mathcal{U}$ and the set of odd integers of $\mathcal{U}$ is represented by 1010100000 $= 1111100000 \wedge 1010101010$.

Definitions

Let A and B be nonempty sets. A **function** f from A to B, denoted $f : A \to B$, also called **mapping** or **transformation**, is an assignment of exactly one element of B to each element of A. If $b \in B$ is the unique element assigned by the function f to the element $a \in A$, this is denoted by $f(a) = b$.

A relation from A to B that contains one, and only one, ordered pair (a, b) for every element $a \in A$, defines a function $f : A \to B$ such that $f(a) = b$ for every ordered pair (a, b). The relation is called the **graph** of the function.

If f is a function from A to B, A is the **domain** of f and B is the **codomain** of f. If $f(a) = b$, b is the **image** of a and a is a **preimage** of b. The **range**, or **image**, of f is the set of all images of elements of A. A function is defined by specifying its domain, its codomain, and the mapping of elements of its domain to (some) elements of its codomain. Two functions are **equal** when their domains, codomains and mappings are the same.

Examples 1–3

The function in Figure 1 has $\{\text{Adams}, \text{Chou}, \text{Goodfriend}, \text{Rodriguez}, \text{Stevens}\}$ as its domain, $\{\text{A}, \text{B}, \text{C}, \text{D}, \text{F}\}$ as its codomain and $\{\text{A}, \text{B}, \text{C}, \text{F}\}$ as its range.

The relation $\{(\text{Abdul}, 22), (\text{Brenda}, 24), (\text{Carla}, 21), (\text{Desire}, 22), (\text{Eddie}, 24), (\text{Felicia}, 22)\}$ specifies a function with domain $\{\text{Abdul}, \text{Brenda}, \text{Carla}, \text{Desire}, \text{Eddie}, \text{Felicia}\}$, range $\{21, 22, 24\}$ and possibly a codomain of positive integers less than 200.

Let f be the function that assigns the 2-bit string consisting the last two bits of a bit string of length 2 or greater. For example, $f(\texttt{11010}) = \texttt{10}$. Then the domain of f is the set of all bit strings of length 2 or greater and the range of f is $\{\texttt{00}, \texttt{01}, \texttt{10}, \texttt{11}\}$.

Examples 4–5

Let $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x^2$. The domain of f is $\mathbb{Z}$, the codomain of f is $\mathbb{Z}$ and the range of f is the set of all integers which are perfect squares, $\{0, 1, 4, 9, \dots\}$.

Domains and codomains of functions are often specified in programming languages. For example, in Java or C, function prototypes such as `int floor(float real)` indicate the domain to be the set of all real numbers represented as `float` values, and the codomain to be the set of all integers represented as `int` values.

A function is called **real-valued** if its codomain is the set of real numbers. A function is called **integer-valued** if its codomain is the set of integers.

Let f_1 and f_2 be real-valued or integer-valued, with a common domain. Then $f_1 + f_2$ and $f_1 f_2$ are also real-valued or integer-valued functions, with the same domain, defined by $(f_1 + f_2)(x) = f_1(x) + f_2(x)$ and $(f_1 f_2)(x) = f_1(x) f_2(x)$.

Image of a Subset

Let $f : A \to B$ and $S \subseteq A$. The **image** of S under the function f, denoted by $f(S)$, is the subset of B that consists of the images of the elements of S. Thus,
$f(S) = \{t \mid \exists s \in S(t = f(s))\} = \{f(s) \mid s \in S\} \subseteq B$.
Let $A = \{a, b, c, d, e\}$ and $B = \{1, 2, 3, 4\}$ with $f(a) = 2$, $f(b) = 1$, $f(c) = 4$, $f(d) = 1$ and $f(e) = 1$. The image of the subset $S = \{b, c, d\}$ is the set $f(S) = \{1, 4\}$.

One-to-One Functions

A function f is said to be **one-to-one**, or an **injunction**, if and only if $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f. A function is said to be **injective** if it is one-to-one. Note that f is injective if and only if $f(a) \neq f(b)$ whenever $a \neq b$.

The function $f : \{a, b, c, d\} \to \{1, 2, 3, 4, 5\}$ where $f(a) = 4$, $f(b) = 5$, $f(c) = 1$ and $f(d) = 3$ is one-to-one. The function $f(x) = x^2$, $f : \mathbb{Z} \to \mathbb{Z}$, is not one-to-one, since $f(1) = f(-1) = 1$. The function $f(x) = x + 1$, $f : \mathbb{R} \to \mathbb{R}$, is one-to-one.

A function f whose domain and codomain are subsets of the set of real numbers is called **increasing** if $f(x) \leq f(y)$ and **strictly increasing** if $f(x) < f(y)$ whenever $x < y$ and x and y are in the domain of f. Similarly, f is called **decreasing** if $f(x) \geq f(y)$ and **strictly decreasing** if $f(x) > f(y)$ whenever $x < y$ and x and y are in the domain of f. If a function is strictly increasing or strictly decreasing, then it is one-to-one.

Onto Functions and Bijections

$f : A \to B$ is called **onto**, or a **surjection**, if and only if, for every element $b \in B$, there is an element $a \in A$ with $f(a) = b$. A function f is called **surjective** if it is onto.

The function $f : \{a, b, c, d\} \to \{1, 2, 3\}$ where $f(a) = 3$, $f(b) = 2$, $f(c) = 1$ and $f(d) = 3$ is onto. The function $f(x) = x^2$, $f : \mathbb{Z} \to \mathbb{Z}$, is not onto, since there is no integer x such that $f(x) = -1$. The function $f(x) = x + 1$, $f : \mathbb{R} \to \mathbb{R}$, is onto.

The function f is a **one-to-one correspondence**, or a **bijection** if it is both one-to-one and onto. We also say such a function is **bijective**.

The function $f : \{a, b, c, d\} \to \{1, 2, 3, 4\}$ where $f(a) = 4$, $f(b) = 2$, $f(c) = 1$ and $f(d) = 3$ is a bijection. If $f : A \to A$ and A is finite, then f is one-to-one if and only if it is onto—this is not necessarily true if A is infinite. The identity function $\iota_A : A \to A$, $\iota_A(x) = x$ is a bijection.

Proving Function Properties

- To show f is injective: show that if $f(x) = f(y)$ for arbitrary x, y in the domain, then $x = y$.
- To show f is not injective: find particular elements x, y in the domain such that $x \neq y$ and $f(x) = f(y)$.
- To show f is surjective: consider an arbitrary element y in the codomain and find its preimage x in the domain such that $f(x) = y$.
- To show f is not surjective: find a particular element y in the codomain such that $f(x) \neq y$ for all elements x of the domain.

Inverse Functions

Let f be a one-to-one correspondence, $f : A \to B$. The **inverse function** of f, denoted f^{-1}, is the function that assigns to an element $b \in B$ the unique element $a \in A$ such that $f(a) = b$—that is, $f^{-1}(b) = a$. As such, a bijective function is called **invertible**.

The function $f : \{a, b, c\} \to \{1, 2, 3\}$ where $f(a) = 2$, $f(b) = 3$ and $f(c) = 1$ is invertible, with $f^{-1}(1) = c$, $f^{-1}(2) = a$ and $f^{-1}(3) = b$. $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x + 1$ is invertible, with $f^{-1}(x) = x - 1$. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ is not invertible, as it is neither one-to-one nor onto. Restricting $f(x) = x^2$ to the domain and codomain of all nonnegative real numbers is invertible, with $f^{-1}(x) = \sqrt{x}$.

Composition of Functions

Let $g : A \to B$ and $f : B \to C$. The **composition** of the functions f and g, denoted by $f \circ g$, is a function defined by $(f \circ g)(a) = f(g(a))$. Note that $f \circ g : A \to C$ cannot be defined unless the range of g is a subset of the domain of f.

Let $g : \{a, b, c\} \to \{a, b, c\}$ with $g(a) = b$, $g(b) = c$ and $g(c) = a$, and $f : \{a, b, c\} \to \{1, 2, 3\}$ with $f(a) = 3$, $f(b) = 2$ and $f(c) = 1$. Then $f \circ g : \{a, b, c\} \to \{1, 2, 3\}$ with $(f \circ g)(a) = 2$, $(f \circ g)(b) = 1$ and $(f \circ g)(c) = 3$, and $g \circ f$ is not defined.

Let $f, g : \mathbb{Z} \to \mathbb{Z}$, $f(x) = 2x + 3$ and $g(x) = 3x + 2$, then $(f \circ g)(x) = 6x + 7$ and $(g \circ f)(x) = 6x + 11$.

If $f : A \to B$ is bijective, $f \circ f^{-1} = \iota_B$ and $f^{-1} \circ f = \iota_A$, identity functions. Also, $(f^{-1})^{-1} = f$.

Floor and Ceiling Functions

The **floor function** or **greatest integer function** assigns to $x \in \mathbb{R}$ the largest integer that is less than or equal to x—this is denoted $x \geq \lfloor x \rfloor = [\![x]\!] \in \mathbb{Z}$. The **ceiling function** assigns to $x \in \mathbb{R}$ the smallest integer that is greater than or equal to x—this is denoted $x \leq \lceil x \rceil \in \mathbb{Z}$. $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$ 100 bits can be encoded in $\lceil 100/8 \rceil = 13$ bytes. ATM data is organized in cells of 53 bytes. In one minute, $\lfloor (500 \cdot 60 \cdot 1000)/(53 \cdot 8) \rfloor = 70754$ cells can be streamed over a 500kilobit / second connection.

- $\lfloor x \rfloor = n$ if and only if $n \leq x < n + 1$ if and only if $x - 1 < n \leq x$
- $\lceil x \rceil = n$ if and only if $n - 1 < x \leq n$ if and only if $x \leq n < x + 1$
- $\lfloor -x \rfloor = -\lceil x \rceil$ and $\lceil -x \rceil = -\lfloor x \rfloor$
- $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ and $\lceil x + n \rceil = \lceil x \rceil + n$
- $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$

Partial Functions

A **partial function** f from a set A to a set B is an assignment to each element a is a subset of A, called the **domain of definition** of f, of a unique element $b \in B$. The sets A and B are called the **domain** and **codomain** of f, respectively. f is said to be **undefined** for elements in A that are not in the domain of definition of f. When the domain of definition of f equals A, f is called a **total function**.

$f(x) = \sqrt{x}$ is a partial function from $\mathbb{Z}$ to $\mathbb{R}$ that is undefined for negative integers. $f(n) = n!$ is a partial function from $\mathbb{Z}$ to $\mathbb{Z}$ that is undefined for negative integers—also, $n! \sim \sqrt{2\pi n}(n/e)^n$.

Cardinality

A set S is finite with cardinality $n \in \mathbb{N}$ if there is a bijection from the set $\{0, 1, \ldots, n-1\}$ to S. A set is infinite if it is not finite.

$\mathbb{N}$ is an infinite set.

The sets A and B have the same cardinality, denoted $|A| = |B|$, if and only if there is a one-to-one correspondence from A to B.

If there is a one-to-one function from A to B, the cardinality of A is less than of the same as the cardinality of B, denoted $|A| \leq |B|$. When $|A| \leq |B|$ and A and B have different cardinality, the cardinality of A is less than the cardinality of B, denoted $|A| < |B|$.

Countable Sets

A set that is eitehr finite or has the same cardinality as the set of positive integers is called **countable**. A set that is not countable is called **uncountable**. When an infinite set S is countable, $|S| = \aleph_0$, and S has cardinality "aleph null".

The set of odd positive integers is a countable set.

An infinite set is countable if and only if it is possible to list the elements of the set in a sequence (indexed by the positive integers).

$\mathbb{Z}$ is countable.

$\mathbb{Q}^+$ is countable.

$\mathbb{R}$ is not countable.

Schröder-Bernstein Theorem

If A and B are countable sets, then $A \cup B$ is also countable.
If A and B are sets with $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$. In other words, if there are one-to-one functions $f : A \to B$ and $g : B \to A$, then there is as one-to-one correspondence between A and B.
$|(0,1)| = |(0,1]|$.
Let S be a set. An **enumeration** of S is a surjective function f from an initial segment of $\mathbb{N}$ to S. If f is injective also, then f is an enumeration without repetitions, otherwise it is an enumeration with repetitions.
If $S = \{\alpha, \beta, \gamma, \delta\}$, then $\langle \alpha, \beta, \gamma, \delta \rangle$ is an enumeration, $\langle \alpha, \gamma, \beta, \beta, \delta, \alpha \rangle$ is an enumeration with repetitions, $\langle \gamma, \alpha, \delta, \beta \rangle$ is an enumeration without repetition.
S is countable if and only if there exists an enumeration of S.
Let $\Sigma = \{a, b\}$. The set of strings over Σ^* is a countably infinite set.

More Results

Every infinite set contains a countably infinite subset.

The union of a countable collection of countable sets is countable.

Let Σ be a finite alphabet and Σ^* the set of all strings over Σ. Then $\mathcal{P}(\Sigma^*)$ is uncountable.

A set S is of cardinality c if there is a bijection from $[0,1]$ (called a **continuum**) to S.

Sets S and T are **equipotent**, or $|S| = |T|$, if there is a bijection from S to T.

Equipotence is an equivalence relation over any collection of sets.

$|S| \leq |T|$ if there exists an injection from S to T. $|S| < |T|$ if there exists an injection but no bijection from S to T.

Continuum Hypothesis and Uncomputable Functions

Let S be a finite set. Then $|S| < \aleph_0 < c$.
If S is an infinite set, then $\aleph_0 \leq |S|$.
Let S be a set. Then $|S| < |\mathcal{P}(S)|$. From there,
$\aleph_0 = |\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \cdots$.
The **continuum hypothesis** says that there is no cardinal number between $\aleph_0$ and c. It was stated by Georg Cantor in 1877, was the first problem posed by David Hilbert in his famous 1900 list of open problems in mathematics, is still an open question and an area for active research.
A function is **computable** if there is a computer program in some programming language that finds the values of this function, otherwise it is **uncomputable**.