Discrete Mathematics, Chapters 2 and 9: Sets, Relations and Functions, Sequences, Sums, Cardinality of Sets

Richard Mayr

University of Edinburgh, UK

Outline

Set Theory

- Basic building block for types of objects in discrete mathematics.
- Set operations in programming languages: Issues about data structures used to represent sets and the computational cost of set operations.
- Set theory is the foundation of mathematics.
- Many different systems of axioms have been proposed.
  Zermelo-Fraenkel set theory (ZF) is standard.
  Often extended by the axiom of choice to ZFC.
- Here we are not concerned with a formal set of axioms for set theory. Instead, we will use what is called naive set theory.

Sets

- A set is an **unordered** collection of objects, e.g., students in this class; air molecules in this room.
- The objects in a set are called the elements, or members of the set. A set is said to contain its elements.
- The notation $x \in S$ denotes that x is an element of the set S.
- If x is not a member of S, write $x \notin S$.

Describing a Set: Roster Method

- $S = \{a, b, c, d\}$.
- Order not important $S = \{a, b, c, d\} = \{b, c, a, d\}$.
- Each distinct object is either a member or not; listing more than once does not change the set. $S = \{a, b, c, d\} = \{a, b, c, b, c, d\}$.
- Dots "$\ldots$" may be used to describe a set without listing all of the members when the pattern is clear. $S = \{a, b, c, d, \ldots, z\}$ or $S = \{5, 6, 7, \ldots, 20\}$.
- Do not overuse this. Patters are not always as clear as the writer thinks.

Some Important Sets

$\mathbb{B}$ = Boolean values = $\{$*true*, *false*$\}$
$\mathbb{N}$ = natural numbers = $\{0, 1, 2, 3, \dots\}$
$\mathbb{Z}$ = integers = $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
$\mathbb{Z}^+ = \mathbb{Z}_{\geq 1}$ = positive integers = $\{1, 2, 3, \dots\}$
$\mathbb{R}$ = set of real numbers
$\mathbb{R}^+ = \mathbb{R}_{>0}$ = set of positive real numbers
$\mathbb{C}$ = set of complex numbers
$\mathbb{Q}$ = set of rational numbers

Set Builder Notation

- Specify the property (or properties) that all members of the set must satisfy.
  $S = \{x \mid x \text{ is a positive integer less than } 100\}$
  $S = \{x \mid x \in \mathbb{Z}^+ \ \wedge \ x < 100\}$
  $S = \{x \in \mathbb{Z}^+ \mid x < 100\}$
- A predicate can be used, e.g.,

  $$S = \{x \mid P(x)\}$$

  where $P(x)$ is true iff x is a prime number.
- Positive rational numbers

  $$\mathbb{Q}^+ = \{x \in \mathbb{R} \mid \exists p, q \in \mathbb{Z}^+ \ x = p/q\}$$

Interval Notation

Used to describe subsets of sets upon which an order is defined, e.g., numbers.

$$[a, b] = \{x \mid a \leq x \leq b\}$$

$$[a, b) = \{x \mid a \leq x < b\}$$

$$(a, b] = \{x \mid a < x \leq b\}$$

$$(a, b) = \{x \mid a < x < b\}$$

closed interval $[a, b]$
open interval (a, b)
half-open intervals $[a, b)$ and $(a, b]$

Universal Set and Empty Set

- The universal set U is the set containing everything currently under consideration.
  - Content depends on the context.
  - Sometimes explicitly stated, sometimes implicit.
- The empty set is the set with no elements.
  Symbolized by $\emptyset$ or $\{\}$.

Russell's Paradox

(After Bertrand Russell (1872–1970); Logician, mathematician and philosopher. Nobel Prize in Literature 1950.)
Naive set theory contains contradictions.

- Let S be the set of all sets which are not members of themselves.

  $$S = \{S' \mid S' \notin S'\}$$

  "Is S a member of itself?", i.e., $S \in S$?
- Related formulation:
  "The barber shaves all people who do not shave themselves, but no one else. Who shaves the barber?"
- Modern formulations (such as Zerlemo-Fraenkel) avoid such obvious problems by stricter axioms about set construction. However, it is impossible to prove in ZF that ZF is consistent (unless ZF is inconsistent).

Things to remember

- Sets **can** be elements of other sets, e.g.,

$$\{\{1, 2, 3\}, a, \{u\}, \{b, c\}\}$$

- The empty set is different from the set containing the empty set

$$\emptyset \neq \{\emptyset\}$$

Subsets and Set Equality

Definition

Set A is a subset of set B iff every element of A is also an element of B. Formally: $A \subseteq B \leftrightarrow \forall x(x \in A \to x \in B)$

In particular, $\emptyset \subseteq S$ and $S \subseteq S$ for every set S.

Definition

Two sets A and B are equal iff they have the same elements. Formally: $A = B \leftrightarrow A \subseteq B \wedge B \subseteq A$.

E.g., $\{1, 5, 5, 5, 3, 3, 1\} = \{1, 3, 5\} = \{3, 5, 1\}$.

Proper Subsets

Definition

A is a **proper subset** of B iff $A \subseteq B$ and $A \neq B$. This is denoted by $A \subset B$.

$A \subset B$ can be expressed by

$$\forall x(x \in A \to x \in B) \ \wedge \ \exists x(x \in B \wedge x \notin A)$$

Set Cardinality

Definition

If there are exactly n distinct elements in a set S, where n is a nonnegative integer, we say that S is finite. Otherwise it is infinite.

Definition

The cardinality of a finite set S, denoted by $|S|$, is the number of (distinct) elements of S.

Examples:

- $|\emptyset| = 0$
- Let S be the set of letters of the English alphabet. Then $|S| = 26$.
- $|\{1, 2, 3\}| = 3$
- $|\{\emptyset\}| = 1$
- The set of integers $\mathbb{Z}$ is infinite.

Power Sets

Definition

The set of all subsets of a set S is called the **power set** of S.
It is denoted by $P(S)$ or 2^S.
Formally: $P(S) = \{S' \mid S' \subseteq S\}$

In particular, $S \in P(S)$ and $\emptyset \in P(S)$.
Example:

$$P(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

If $|S| = n$ then $|P(S)| = 2^n$. Proof by induction on n; see later Chapters.

Tuples

- The ordered n-tuple $(a_1, a_2, \ldots, a_n)$ is the ordered collection of n elements, where a_1 is the first, a_2 the second, etc., and a_n the n-th (i.e., the last).
- Two n-tuples are equal iff their corresponding elements are equal.

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \leftrightarrow a_1 = b_1 \wedge a_2 = b_2 \wedge \cdots \wedge a_n = b_n$$

- 2-tuples are called ordered pairs.

Cartesian Product

Definition

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

Definition

The Cartesian product of n sets $A_1, A_2 \dots, A_n$, denoted by $A_1 \times A_2 \times \cdots \times A_n$, is the set of all tuples $(a_1, a_2, \dots, a_n)$ where $a_i \in A_i$ for $i = 1, \dots, n$.
$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i \text{ for } i = 1, 2, \dots, n\}$

Example: What is $A \times B \times C$ where $A = \{0, 1\}, B = \{1, 2\}$ and $C = \{0, 1, 2\}$.
Solution: $A \times B \times C = \{(0, 1, 0), (0, 1, 1), (0, 1, 2), (0, 2, 0), (0, 2, 1), (0, 2, 2), (1, 1, 0), (1, 1, 1), (1, 1, 2), (1, 2, 0), (1, 2, 1), (1, 1, 2)\}$

Truth Sets and Characteristic Predicates

We fix a domain U.

- Let $P(x)$ be a predicate on U. The truth set of P is the subset of U where P is true.

$$\{x \in U \mid P(x)\}$$

- Let $S \subseteq U$ be a subset of U. The characteristic predicate of S is the predicate P that is true exactly on S, i.e.,

$$P(x) \leftrightarrow x \in S$$

Set Operations: Union, Intersection, Complement

Given a domain U and two sets A, B.

- The union of two sets A, B is defined by
  $A \cup B = \{x \mid x \in A \vee x \in B\}$.
  General union of several sets:
  $A_1 \cup \cdots \cup A_n = \{x \mid x \in A_1 \vee \cdots \vee x \in A_n\}$
- The intersection of two sets A, B is defined by
  $A \cap B = \{x \mid x \in A \wedge x \in B\}$.
  General intersection of several sets:
  $A_1 \cap \cdots \cap A_n = \{x \mid x \in A_1 \wedge \cdots \wedge x \in A_n\}$
- The complement of A **w.r.t.** U is defined by

$$\overline{A} = \{x \in U \mid x \notin A\}$$

Set Difference

Definition

The difference between sets A and B, denoted $A - B$ is the set containing the elements of A that are not in B. Formally:
$A - B = \{x \mid x \in A \wedge x \notin B\} = A \cap \overline{B}$

$A - B$ is also called the complement of B w.r.t. A.

Definition

The **symmetric difference** between sets A and B, denoted $A \triangle B$ is the set containing the elements of A that are not in B or vice-versa.
Formally:
$A \triangle B = \{x \mid x \in A \text{ } xor \text{ } x \in B\} = (A - B) \cup (B - A)$

$A \triangle B = (A \cup B) - (A \cap B)$.

Cardinality of Finite Derived Sets

- $|A \cup B| = |A| + |B| - |A \cap B|$
  In particular, $|A \cup B| \leq |A| + |B|$.
- $|A \cap B| \leq |A|$
  $|A \cap B| \leq |B|$
- $|A - B| \leq |A|$
- $|A \triangle B| = ?$

Clicker

1. $|A| + |B|$
2. $|A| + |B| - |A \cap B|$
3. $|A| + |B| - 2|A \cap B|$
4. $|A| + |B| + |A \cap B|$
5. $|A| + |B| + 2|A \cap B|$
6. $|A| + |B| - |A \cup B|$

Cardinality of Finite Derived Sets

- $|A \cup B| = |A| + |B| - |A \cap B|$
  In particular, $|A \cup B| \leq |A| + |B|$.
- $|A \cap B| \leq |A|$
  $|A \cap B| \leq |B|$
- $|A - B| \leq |A|$
- $|A \triangle B| = ?$

Clicker

1. $|A| + |B|$
2. $|A| + |B| - |A \cap B|$
3. $|A| + |B| - 2|A \cap B|$
4. $|A| + |B| + |A \cap B|$
5. $|A| + |B| + 2|A \cap B|$
6. $|A| + |B| - |A \cup B|$

$|A| + |B| - 2|A \cap B|$

Set Identities

- Identity laws
$$A \cup \emptyset = A \quad A \cap U = A$$
- Domination laws
$$A \cup U = U \quad A \cap \emptyset = \emptyset$$
- Idempotent laws
$$A \cup A = A \quad A \cap A = A$$
- Complementation law
$$\overline{(\overline{A})} = A$$
- Complement laws
$$A \cap \overline{A} = \emptyset \quad A \cup \overline{A} = U$$

Set Identities (cont.)

- Commutative laws

$$A \cup B = B \cup A \quad A \cap B = B \cap A$$

- Associative laws
  $A \cup (B \cup C) = (A \cup B) \cup C$
  $A \cap (B \cap C) = (A \cap B) \cap C$
- Distributive laws
  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- Absorption laws

$$A \cup (A \cap B) = A \quad A \cap (A \cup B) = A$$

- De Morgan's laws

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \quad \overline{A \cap B} = \overline{A} \cup \overline{B}$$

Relations

Definition

Given sets $A_1, \ldots, A_n$, a subset $R \subseteq A_1 \times \cdots \times A_n$ is an n-ary relation.

Example: Database R contains tuples (Street name, House number, currently inhabited flag), i.e., $R \subseteq \mathit{Strings} \times \mathbb{N} \times \mathbb{B}$. So R is a 3-ary relation.

Definition

Given sets A and B, $R \subseteq A \times B$ is a binary relation from A to B.

The property $(x, y) \in R$ is also written as xRy.
Example: $R \subseteq \mathbb{R} \times \mathbb{Z}$ where $(x, y) \in R$ iff $y = \lfloor x \rfloor$ (rounding down).

Definition

$R \subseteq A \times A$ is called a relation on A.

Example: $\leq \subseteq \mathbb{Z} \times \mathbb{Z}$ is the 'less or equal' relation on the integers.

Relations and Matrices

- A binary relation $R \subseteq A \times B$ can be described by a boolean matrix (and vice-versa).
- Define a boolean matrix M. Index its rows over set A and its columns of set B.
- Let $M(a, b) = \mathbf{T}$ iff $(a, b) \in R$.

Properties of Binary Relations

A binary relation $R \subseteq A \times A$ is called

- Reflexive iff $\forall x\, (x, x) \in R$
- Symmetric iff $\forall x, y\, ((x, y) \in R \rightarrow (y, x) \in R)$
- Antisymmetric iff $\forall x, y\, ((x, y) \in R \wedge (y, x) \in R \rightarrow x = y)$
- Transitive iff $\forall x, y, z\, ((x, y) \in R \wedge (y, z) \in R \rightarrow (x, z) \in R)$.

Examples:

- $\leq$ and $=$ are reflexive, but $<$ is not.
- $=$ is symmetric, but $\leq$ is not.
- $\leq$ is antisymmetric.
  Note: $=$ is also antisymmetric, i.e., $=$ is symmetric and antisymmetric.
  $<$ is also antisymmetric, since the precondition of the implication is always false.
  However, $R = \{(x, y) \mid x + y \leq 3\}$ is not antisymmetric, since $(1, 2), (2, 1) \in R$.
- All three, $=$, $\leq$ and $<$ are transitive.
  $R = \{(x, y) \mid y = 2x\}$ is not transitive.

Binary Relations: Example

Let

$$R = \{(x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid \exists k \in \mathbb{Z}^+ y = kx\}$$

Clicker: Is R

1. reflexive, symmetric, transitive
2. not reflexive, antisymmetric, not transitive
3. reflexive, not antisymmetric, transitive
4. reflexive, symmetric, not transitive
5. reflexive, antisymmetric, transitive
6. reflexive, not symmetric, not transitive

Combining Relations

Since relations are sets, they can be combined with normal set operations, e.g., $< \cup =$ is equal to $\leq$, and $\leq \cap \geq$ is equal to $=$.
Moreover, relations can be composed.

Definition

Let $R_1 \subseteq A \times B$ and $R_2 \subseteq B \times C$. Then R_1 is composable with R_2.
The composition is defined by

$$R_1 \circ R_2 = \{(x,z) \in A \times C \mid \exists y \in B\, ((x,y) \in R_1 \land (y,z) \in R_2)\}$$

Sometimes $R_1 \circ R_2$ is simply written as $R_1 R_2$.
Example: If $A, B, C = \mathbb{Z}$ then

$$> \circ > = \qquad .$$

However if $A, B, C = \mathbb{R}$ then

$$> \circ > =$$

Combining Relations

Since relations are sets, they can be combined with normal set operations, e.g., $< \cup =$ is equal to $\leq$, and $\leq \cap \geq$ is equal to $=$.
Moreover, relations can be composed.

Definition

Let $R_1 \subseteq A \times B$ and $R_2 \subseteq B \times C$. Then R_1 is composable with R_2.
The composition is defined by

$$R_1 \circ R_2 = \{(x,z) \in A \times C \mid \exists y \in B\, ((x,y) \in R_1 \wedge (y,z) \in R_2)\}$$

Sometimes $R_1 \circ R_2$ is simply written as $R_1 R_2$.
Example: If $A, B, C = \mathbb{Z}$ then

$$> \circ > = \ \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x \geq y + 2\}.$$

However if $A, B, C = \mathbb{R}$ then

$$> \circ > =$$

Combining Relations

Since relations are sets, they can be combined with normal set operations, e.g., $< \cup =$ is equal to $\leq$, and $\leq \cap \geq$ is equal to $=$.
Moreover, relations can be composed.

Definition

Let $R_1 \subseteq A \times B$ and $R_2 \subseteq B \times C$. Then R_1 is composable with R_2.
The composition is defined by

$$R_1 \circ R_2 = \{(x,z) \in A \times C \mid \exists y \in B\, ((x,y) \in R_1 \wedge (y,z) \in R_2)\}$$

Sometimes $R_1 \circ R_2$ is simply written as $R_1 R_2$.
Example: If $A, B, C = \mathbb{Z}$ then

$$> \circ > = \ \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x \geq y + 2\}.$$

However if $A, B, C = \mathbb{R}$ then

$$> \circ > = \ >$$

Powers of a Relation

Definition

Given a relation $R \subseteq A \times A$ on A, its powers are defined inductively by

Base step: $R^1 = R$

Induction step: $R^{n+1} = R^n \circ R$

If R is a transitive relation, then its powers are contained in R itself. Moreover, the reverse implication also holds.

Theorem

A relation R on a set A is transitive iff $R^n \subseteq R$ for all $n = 1, 2, \dots$.

Proof by induction on n.

Equivalence Relations

Definition

A relation R on a set A is called an **equivalence relation** iff it is reflexive, symmetric and transitive.

Example: Let Σ^* be the set of strings over alphabet Σ. Let $R \subseteq \Sigma^* \times \Sigma^*$ be a relation on strings defined as follows. $R = \{(s,t) \in \Sigma^* \times \Sigma^* \mid |s| = |t|\}$. I.e., two strings are in relation iff they have the same length.
Verify that R is an equivalence relation. Prove that it is reflexive, symmetric and transitive.

Example: Let $R = \{(a,b) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid a \text{ divides } b\}$. This is not an equivalence relation. It is reflexive and transitive, but not symmetric.

Congruence modulo m

Let $m > 1$ be an integer. Show that the relation

$$R = \{(a, b) \mid a \equiv b(\mod m)\}$$

is an equivalence on the set of integers.

Proof: Recall that $a \equiv b(\mod m)$ iff m divides $a - b$.

Reflexivity: $a \equiv a(\mod m)$ since $a - a = 0$ is divisible by m.

Symmetry: Suppose $(a, b) \in R$. Then m divides $a - b$. Thus there exists some integer k s.t. $a - b = km$. Therefore $b - a = (-k)m$. So m divides $b - a$ and thus $b \equiv a(\mod m)$, and finally $(b, a) \in R$.

Transitivity: If $(a, b) \in R$ and $(b, c) \in R$ then $a \equiv b(\mod m)$ and $b \equiv c(\mod m)$. So m divides both $a - b$ and $b - c$. Hence there exist integers k, l with $a - b = km$ and $b - c = lm$. By adding these two equations we obtain $a - c = (a - b) + (b - c) = km + lm = (k + l)m$. Therefore, $a \equiv c(\mod m)$ and $(a, c) \in R$.

Equivalence Classes

Definition

Let R be an equivalence relation on a set A and $a \in A$ an element of A. Let

$$[a]_R = \{s \mid (a, s) \in R\}$$

be the equivalence class of a w.r.t. R, i.e., all elements of A that are R-equivalent to a.

If $b \in [a]_R$ then b is called a representative of the equivalence class. Every member of the class can be a representative.

Theorem

Let R be an equivalence on A and $a, b \in A$. The following three statements are equivalent.

1. aRb
2. $[a] = [b]$
3. $[a] \cap [b] \neq \emptyset$.

Partitions of a Set

Definition

A partition of a set A is a collection of disjoint, nonempty subsets that have A as their union. In other words, the collection of subsets $A_i \subseteq A$ with $i \in I$ (where I is an index set) forms a partition of A iff

1. $A_i \neq \emptyset$ for all $i \in I$.
2. $A_i \cap A_j = \emptyset$ for $i \neq j$
3. $\bigcup_{i \in I} A_i = A$

Theorem

- *If R is an equivalence on A, then the equivalence classes of R form a partition of A.*
- *Conversely, given a partition $\{A_i \mid i \in I\}$ of A there exists an equivalence relation R that has exactly the sets A_i, $i \in I$, as its equivalence classes.*

Partial Orders

Definition

A relation R on a set A is called a **partial order** iff it is reflexive, antisymmetric and transitive.
If R is a partial order, we call (A, R) a partially ordered set, or poset.

Example: $\leq$ is a partial order, but $<$ is not (since it is not reflexive).

Example: Let $a|b$ denote the fact that a divides b. Formally: $\exists k \in \mathbb{Z}\ ak = b$. Show that the relation $|$ is a partial order, i.e., $(\mathbb{Z}^+, |)$ is a poset.

Example: Set inclusion $\subseteq$ is partial order, i.e., $(2^A, \subseteq)$ is a poset.

Comparability and Total Orders

Definition

Two elements a and b of a poset (S, R) are called **comparable** iff aRb or bRa holds. Otherwise they are called **incomparable**.

Definition

If (S, R) is a poset where every two elements are comparable, then S is called a **totally ordered** or **linearly ordered** set and the relation R is called a **total order** or **linear order**.

A totally ordered set is also called a chain.

Given a poset (S, R) and $S' \subseteq S$ a subset in which all elements are pairwise incomparable. Then S' is called an antichain.

Extending Orders to Tuples/Vectors: Standard

Let $(S, \preccurlyeq)$ be a poset and $S^n = S \times S \times \cdots \times S$ (n times).
The standard extension of the partial order to tuples in S^n is defined by

$$(x_1, \ldots, x_n) \preccurlyeq (y_1, \ldots, y_n) \;\leftrightarrow\; \forall i \in \{1, \ldots, n\}\, x_i \preccurlyeq y_i$$

Exercise: Prove that this defines a partial order.

Note: Even if $(S, \preccurlyeq)$ is totally ordered, the extension to S^n is not necessarily a total order. Consider $(\mathbb{N}, \leq)$. Then $(2,1) \npreceq (1,2) \npreceq (2,1)$.

Extending Orders to Tuples/Vectors: Lexicographic

Let $(S, \preccurlyeq)$ be a poset and $S^n = S \times S \times \cdots \times S$ (n times).
The lexicographic order on tuples in S^n is defined by

$$(x_1, \ldots, x_n) \prec_{lex} (y_1, \ldots, y_n) \leftrightarrow \exists i \in \{1, \ldots, n\} \forall k < i\, x_k = y_k \wedge x_i \prec y_i$$

Let $(x_1, \ldots, x_n) \preccurlyeq_{lex} (y_1, \ldots, y_n)$ iff $(x_1, \ldots, x_n) \prec_{lex} (y_1, \ldots, y_n)$ or $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$.

Lemma

If $(S, \preccurlyeq)$ is totally ordered then $(S^n, \preccurlyeq_{lex})$ is totally ordered.

Functions as Relations

Definition

Let A, B be nonempty sets. A relation $f \subseteq A \times B$ is called a **partial function** from A to B iff it satisfies the function condition

$$(a, b) \in f \wedge (a, c) \in f \ \rightarrow \ b = c$$

I.e., f assigns every element $a \in A$ at most one element in B.
Partial functions from A to B are denoted as $f : A \rightarrow B$, and we write $f(a) = b$ instead of $(a, b) \in f$.
Functions are also called mappings or transformations.

Definition

A partial function $f : A \rightarrow B$ is called a **total function** iff every element in A is assigned an element in B, i.e., $\forall a \in A \exists b \in B\ (a, b) \in f$.

Terminology about Functions

Let $f : A \to B$ be a function from A to B.

- We say that f maps A to B.
- A is called the domain of f.
- B is called the codomain of f.
- If $f(a) = b$ then b is the image of a under f and a is the preimage of b.
- $f(A) := \{b \in B \mid \exists a \in A\, f(a) = b\}$ is called the range of f. (Note the difference between the range and the codomain.)
- Two functions $f : A \to B$ and $g : A' \to B'$ are equal iff $A = A'$, $B = B'$ and $\forall a \in A\, f(a) = g(a)$.

Representing Functions

Functions can be specified in different ways:

- Explicit statement of assignments, e.g., $f(2) = 4$, $f(3) = 1$, $f(4) = 17$.
- A formula, e.g., $f(x) = 5x^2 - 3x + 12$.
- An algorithm/program, e.g., If x is odd and $x > 17$ then $f(x) = 5$ else if x is even then $f(x) = x/2$, otherwise $f(x) = 3x$.
- General conditions on a function that have just one unique solution.

Injections, Surjections, Bijections

Definition

A function $f : A \to B$ is **injective** ("one-to-one") iff $f(a) = f(b) \to a = b$. Then f is called an **injection**.

Definition

A function $f : A \to B$ is **surjective** ("onto") iff $\forall b \in B \, \exists a \in A \; f(a) = b$. Then f is called a **surjection**.

A function $f : A \to B$ is surjective iff $f(A) = B$, i.e., the range is equal to the codomain.

Definition

A function $f : A \to B$ is **bijective** iff it is injective and surjective. Then f is called a **bijection** or **one-to-one correspondence**.

Reasoning about Injections, Surjections

Suppose that $f : A \to B$.

To show that f is injective Show that if $f(x) = f(y)$ for arbitrary $x, y \in A$ with $x \neq y$, then $x = y$.

To show that f is not injective Find particular elements $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$.

To show that f is surjective Consider an arbitrary element $y \in B$ and find an element $x \in A$ such that $f(x) = y$.

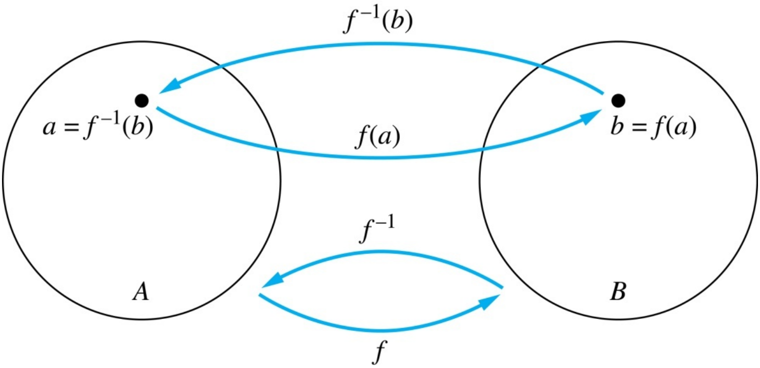
To show that f is not surjective Find a particular $y \in B$ such that $f(x) \neq y$ for all $x \in A$.

Inverse Function

Definition

If $f : A \to B$ is a bijection then the **inverse** of f, denoted by f^{-1} is defined as the function $f^{-1} : B \to A$ s.t. $f^{-1}(b) = a$ iff $f(a) = b$.

If f is not a bijection then the inverse does not exist.



Examples

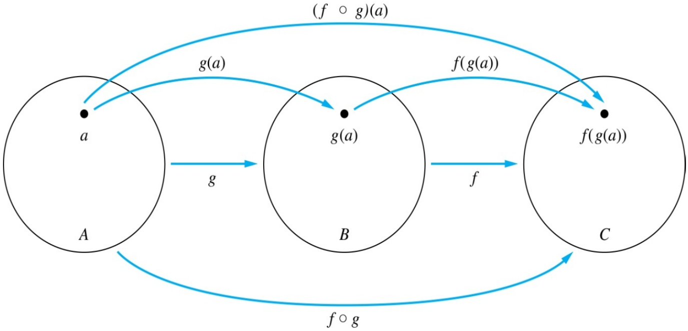
Does the inverse of the following functions exist? Why (not)?

- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x + 1$
- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$
- $f : \mathbb{N} \to \mathbb{N}$, $f(x) = 2x$
- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x$

Function Composition

Definition

Let $f : B \to C$ and $g : A \to B$. The composition function $f \circ g$ is defined by $f \circ g : A \to C$ with $f \circ g(a) = f(g(a))$.



(The common notation differs between functions and relations. For functions $f \circ g$ normally means "first apply g, then apply f". For relations it is vice-versa: $R_1 \circ R_2$ means "first R_1, then R_2"; see above.)

Floor and Ceiling Functions

TABLE 1 Useful Properties of the Floor and Ceiling Functions. (n is an integer, x is a real number)	
(1a)	$\lfloor x \rfloor = n$ if and only if $n \leq x < n + 1$
(1b)	$\lceil x \rceil = n$ if and only if $n - 1 < x \leq n$
(1c)	$\lfloor x \rfloor = n$ if and only if $x - 1 < n \leq x$
(1d)	$\lceil x \rceil = n$ if and only if $x \leq n < x + 1$
(2)	$x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$
(3a)	$\lfloor -x \rfloor = -\lceil x \rceil$
(3b)	$\lceil -x \rceil = -\lfloor x \rfloor$
(4a)	$\lfloor x + n \rfloor = \lfloor x \rfloor + n$
(4b)	$\lceil x + n \rceil = \lceil x \rceil + n$

Proving Properties of Functions

Example: Prove that if x is a real number, then $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + 1/2 \rfloor$.
Solution: Let $x = n + \epsilon$, where n is an integer and $0 \leq \epsilon < 1$.

Case 1: $\epsilon < 1/2$.
$2x = 2n + 2\epsilon$ and $\lfloor 2x \rfloor = 2n$, since $0 \leq 2\epsilon < 1$.
$\lfloor x + 1/2 \rfloor = n$, since $x + 1/2 = n + (1/2 + \epsilon)$ and $0 \leq 1/2 + \epsilon < 1$. Hence, $\lfloor 2x \rfloor = 2n$ and $\lfloor x \rfloor + \lfloor x + 1/2 \rfloor = n + n = 2n$.

Case 2: $\epsilon \geq 1/2$
$2x = 2n + 2\epsilon = (2n + 1) + (2\epsilon - 1)$ and $\lfloor 2x \rfloor = 2n + 1$, since $0 \leq 2\epsilon - 1 < 1$.
$\lfloor x + 1/2 \rfloor = \lfloor n + (1/2 + \epsilon) \rfloor = \lfloor n + 1 + (\epsilon - 1/2) \rfloor = n + 1$ since $0 \leq \epsilon - 1/2 < 1$. Hence, $\lfloor 2x \rfloor = 2n + 1$ and $\lfloor x \rfloor + \lfloor x + 1/2 \rfloor = n + (n + 1) = 2n + 1$.

Factorial Function

Definition

The factorial function $f : \mathbb{N} \to \mathbb{N}$, denoted as $f(n) = n!$ assigns to n the product of the first n positive integers.

$$f(0) = 0! = 1$$

and

$$f(n) = n! = 1 \cdot 2 \cdot \dots \cdot (n-1) \cdot n$$

Can be approximated by Stirling's formula:

$$g(n) = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

We have approximately $n! \sim g(n)$ in the sense that $\lim_{n\to\infty} n!/g(n) = 1$ and

$$\sqrt{2\pi}n^{n+1/2}e^{-n} \le n! \le e\, n^{n+1/2}e^{-n}$$

Closure

Definition

A **closure operator** on a set S is a function $C : 2^S \to 2^S$ that satisfies the following conditions for all $X, Y \subseteq S$.

Extensive: $X \subseteq C(X)$

Monotone: $X \subseteq Y \ \to \ C(X) \subseteq C(Y)$

Idempotent: $C(C(X)) = C(X)$

A set X is called closed under C iff $X = C(X)$.
Often closure operators are derived from (one or several) operations on the elements of a set. E.g., the closure under addition is defined as

$$C(X) := X \cup \{a_1 + \cdots + a_k \mid a_1, \ldots, a_k \in X\}$$

$\mathbb{N}$ is closed under addition, but not under subtraction. $3 - 7 = -4 \notin \mathbb{N}$.
$\mathbb{R}$ is closed under multiplication, but not under division.

Closure

Definition

A **closure operator** on a set S is a function $C : 2^S \to 2^S$ that satisfies the following conditions for all $X, Y \subseteq S$.

Extensive: $X \subseteq C(X)$

Monotone: $X \subseteq Y \ \to \ C(X) \subseteq C(Y)$

Idempotent: $C(C(X)) = C(X)$

A set X is called closed under C iff $X = C(X)$.
Often closure operators are derived from (one or several) operations on the elements of a set. E.g., the closure under addition is defined as

$$C(X) := X \cup \{a_1 + \cdots + a_k \mid a_1, \ldots, a_k \in X\}$$

$\mathbb{N}$ is closed under addition, but not under subtraction. $3 - 7 = -4 \notin \mathbb{N}$.
$\mathbb{R}$ is closed under multiplication, but not under division. $1/0 \notin \mathbb{R}$.

Closure (cont.)

- Closure operators can also be defined by properties of sets.
- Let $P : 2^S \rightarrow \{\mathbf{T}, \mathbf{F}\}$ a property of sets.
- Let $C(X)$ be the smallest set Y s.t. $X \subseteq Y$ and $P(Y)$, i.e., the smallest extension of X that satisfies property P.
- This yields a closure operator only if such a smallest Y actually exists.
- Example: Binary relations $R \subseteq S \times S$ are subsets of $S \times S$. Define the transitive closure of relations $C : 2^{S \times S} \rightarrow 2^{S \times S}$ by

$$C(R) := \text{The smallest transitive relation } R' \text{ with } R \subseteq R'$$

- The transitive closure of relations does exist, because the intersection of transitive relations is transitive.
  Thus $C(R) := \bigcap_{R \subseteq R', R' \text{ transitive}} R'$.

Sequences

Sequences are ordered lists of elements, e.g.,
$2, 3, 5, 7, 11, 13, 17, 19, \ldots$ or $a, b, c, d, \ldots$.

Definition

A sequence over a set S is a function f from a subset of the integers (typically $\mathbb{N}$ or $\mathbb{N} - \{0\}$) to the set S.
If the domain of f is finite then the sequence is finite.

Example: Let $f : \mathbb{N} - \{0\} \to \mathbb{Q}$ be defined by $f(n) := 1/n$.
This defines the sequence

$$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$$

Let $a_n = f(n)$. Then the sequence is also written as $a_1, a_2, a_3, \ldots$ or as

$$\{a_n\}_{n \in \mathbb{N} - \{0\}}$$

Geometric vs. Arithmetic Progression

- A geometric progression is a sequence of the form

$$a, ar, ar^2, ar^3, \ldots, ar^n, \ldots$$

where both the initial element a and the common **ratio** r are real numbers.

- An arithmetic progression is a sequence of the form

$$a, a+d, a+2d, a+3d, \ldots, a+nd, \ldots$$

where both the initial element a and the common **difference** d are real numbers.

Recurrence Relations

Definition

A **recurrence relation** for the sequence $\{a_n\}_{n \in \mathbb{N}}$ is an equation that expresses a_n in terms of (one or more of) the previous elements $a_0, a_1, \ldots, a_{n-1}$ of the sequence.

- Typically the recurrence relation expresses a_n in terms of just a fixed number of previous elements, e.g., $a_n = g(a_{n-1}, a_{n-2}) = 2a_{n-1} + a_{n-2} + 7$.
- The initial conditions specify the first elements of the sequence, before the recurrence relation applies.
- A sequence is called a solution of a recurrence relation iff its terms satisfy the recurrence relation.
- Example: Let $a_0 = 2$ and $a_n = a_{n-1} + 3$ for $n \geq 1$. Then $a_1 = 5$, $a_2 = 8$, $a_3 = 11$, etc. Generally the solution is $f(n) = 2 + 3n$.

Fibonacci Sequence

- The Fibonacci sequence is described by the following linear recurrence relation.
- $f(0) = 0$, $f(1) = 1$ and $f(n) = f(n-1) + f(n-2)$ for $n \geq 2$.
- You obtain the sequence $0, 1, 1, 2, 3, 5, 8, 13, \ldots$.
- How to solve general recurrence with
  $f(0) = a, f(1) = b, f(n) = c \cdot f(n-1) + d \cdot f(n-2) \quad ?$
  Linear algebra. Matrix multiplication. Base transforms. Diagonal form., etc.

Solving Recurrence Relations

- Finding a formula for the n-th term of the sequence generated by a recurrence relation is called solving the recurrence relation.
- Such a formula is called a closed formula.
- Various methods for solving recurrence relations will be covered in Chapter 8 where recurrence relations will be studied in greater depth.
- Here we illustrate by example the method of iteration in which we need to guess the formula.
- The guess can be proved correct by the method of induction (Chapter 5).

Iterative Solution Example 1

Method 1: Working upward, forward substitution.
Let a_n be a sequence that satisfies the recurrence relation $a_n = a_{n-1} + 3$ for $n \geq 2$ and suppose that $a_1 = 2$.

$$\begin{aligned} a_2 &= 2 + 3 \\ a_3 &= (2+3) + 3 = 2 + 3 \cdot 2 \\ a_4 &= (2 + 2 \cdot 3) + 3 = 2 + 3 \cdot 3 \end{aligned}$$

$$a_n = a_{n-1} + 3 = (2 + 3 \cdot (n-2)) + 3 = 2 + 3(n-1)$$

Iterative Solution Example 2

Method 2: Working downward, backward substitution.
Let a_n be a sequence that satisfies the recurrence relation $a_n = a_{n-1} + 3$ for $n \geq 2$ and suppose that $a_1 = 2$.

$$\begin{aligned} a_n &= a_{n-1} + 3 \\ &= (a_{n-2} + 3) + 3 = a_{n-2} + 3 \cdot 2 \\ &= (a_{n-3} + 3) + 3 \cdot 2 = a_{n-3} + 3 \cdot 3 \\ \\ &= a_2 + 3(n-2) = (a_1 + 3) + 3(n-2) = 2 + 3(n-1) \end{aligned}$$

Common Sequences

TABLE 1 Some Useful Sequences.

nth Term	*First 10 Terms*
n^2	$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, \ldots$
n^3	$1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, \ldots$
n^4	$1, 16, 81, 256, 625, 1296, 2401, 4096, 6561, 10000, \ldots$
2^n	$2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, \ldots$
3^n	$3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, \ldots$
$n!$	$1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800, \ldots$
f_n	$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

See also The On-Line Encyclopedia of Integer Sequences (OEIS) at http://oeis.org/

Summations

Given a sequence $\{a_n\}$. The sum of the terms $a_m, a_{m+1}, \ldots, a_n$ is written as

$$a_m + a_{m+1} + \cdots + a_n$$

$$\sum_{j=m}^{n} a_j$$

$$\sum_{m \le j \le n} a_j$$

The variable j is called the index of summation. It runs through all the integers starting with its lower limit m and ending with its upper limit n. More generally for an index set S one writes

$$\sum_{j \in S} a_j$$

Useful Summation Formulae

TABLE 2 Some Useful Summation Formulae.

Sum	*Closed Form*
$\sum_{k=0}^{n} ar^k \ (r \neq 0)$	$\frac{ar^{n+1} - a}{r - 1}, r \neq 1$
$\sum_{k=1}^{n} k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=0}^{\infty} x^k, \lvert x \rvert < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{\infty} kx^{k-1}, \lvert x \rvert < 1$	$\frac{1}{(1-x)^2}$

Products

Given a sequence $\{a_n\}$. The product of the terms $a_m, a_{m+1}, \ldots, a_n$ is written as

$$a_m * a_{m+1} * \cdots * a_n$$

$$\prod_{j=m}^{n} a_j$$

$$\prod_{m \leq j \leq n} a_j$$

More generally for an index set S one writes

$$\prod_{j \in S} a_j$$

Counting: Finite Sequences

Given a finite set S with $|S| = k$.
How many different sequences over S of length n are there?
Clicker

1. $k \cdot n$
2. $k + n$
3. n^k
4. k^n
5. $n \cdot k^n$
6. $k \cdot n^k$

Counting: Finite Sequences

Given a finite set S with $|S| = k$.
How many different sequences over S of length n are there?
Answer: For each of the n elements of the sequence there are k possible choices. So the answer is $k * k * \cdots * k$ (n times).
In other words, we get

$$\prod_{1 \leq j \leq n} k = k^n$$

How many sequences over S of length $\leq n$ are there?

Counting: Finite Sequences

Given a finite set S with $|S| = k$.
How many different sequences over S of length n are there?
Answer: For each of the n elements of the sequence there are k possible choices. So the answer is $k * k * \cdots * k$ (n times).
In other words, we get

$$\prod_{1 \le j \le n} k = k^n$$

How many sequences over S of length $\le n$ are there?
Sum over the (non-overlapping!) cases of length $j = 0, 1, 2, \ldots, n$.

$$\sum_{j=0}^{n} k^j = \frac{k^{n+1} - 1}{k - 1}$$

(By the sum formula of the previous slide.)

Counting: Relations and Functions on Finite Sets

Let A and B be **finite** sets, i.e., $|A|$ and $|B|$ are finite.

- What is the size of $A \times B$?
- How many binary relations $R \subseteq A \times B$ from A to B are there?
- How many total functions $f : A \to B$ from A to B are there?

Counting: Relations and Functions on Finite Sets

Let A and B be **finite** sets, i.e., $|A|$ and $|B|$ are finite.

- What is the size of $A \times B$? $|A \times B| = |A| \cdot |B|$
- How many binary relations $R \subseteq A \times B$ from A to B are there?
- How many total functions $f : A \to B$ from A to B are there?

Counting: Relations and Functions on Finite Sets

Let A and B be **finite** sets, i.e., $|A|$ and $|B|$ are finite.

- What is the size of $A \times B$? $|A \times B| = |A| \cdot |B|$
- How many binary relations $R \subseteq A \times B$ from A to B are there? The number of relations from A to B is the number of subsets of $A \times B$. Thus the answer is $2^{|A| \cdot |B|}$.
- How many total functions $f : A \to B$ from A to B are there?

Counting: Relations and Functions on Finite Sets

Let A and B be **finite** sets, i.e., $|A|$ and $|B|$ are finite.

- What is the size of $A \times B$? $|A \times B| = |A| \cdot |B|$
- How many binary relations $R \subseteq A \times B$ from A to B are there? The number of relations from A to B is the number of subsets of $A \times B$. Thus the answer is $2^{|A| \cdot |B|}$.
- How many total functions $f : A \to B$ from A to B are there? A total function f assigns exactly one element from B to every element of A. Thus for every element of $a \in A$ there are $|B|$ possible choices for $f(a) \in B$. Thus the answer is $|B|^{|A|}$.

Counting: Relations and Functions on Finite Sets

Let A and B be **finite** sets, i.e., $|A|$ and $|B|$ are finite.

- What is the size of $A \times B$? $|A \times B| = |A| \cdot |B|$
- How many binary relations $R \subseteq A \times B$ from A to B are there? The number of relations from A to B is the number of subsets of $A \times B$. Thus the answer is $2^{|A| \cdot |B|}$.
- How many total functions $f : A \to B$ from A to B are there? A total function f assigns exactly one element from B to every element of A. Thus for every element of $a \in A$ there are $|B|$ possible choices for $f(a) \in B$. Thus the answer is $|B|^{|A|}$.

The set of all total functions $f : A \to B$ from A to B is denoted by

$$B^A$$

Thus we get that $|B^A| = |B|^{|A|}$.

Cardinality of (Infinite) Sets

The sizes of finite sets are easy to compare.
But what about infinite sets?
Can one infinite set be larger than another?

Cardinality of (Infinite) Sets

The sizes of finite sets are easy to compare.
But what about infinite sets?
Can one infinite set be larger than another?

Definition

- Two sets A and B have the same **cardinality**, written $|A| = |B|$ iff there exists a bijection from A to B.
- We say $|A| \leq |B|$ iff there exists an injection from A to B.
- A has lower cardinality than B, written $|A| < |B|$ iff $|A| \leq |B|$ and $|A| \neq |B|$.

Cardinality of (Infinite) Sets

The sizes of finite sets are easy to compare.
But what about infinite sets?
Can one infinite set be larger than another?

Definition

- Two sets A and B have the same **cardinality**, written $|A| = |B|$ iff there exists a bijection from A to B.
- We say $|A| \leq |B|$ iff there exists an injection from A to B.
- A has lower cardinality than B, written $|A| < |B|$ iff $|A| \leq |B|$ and $|A| \neq |B|$.

Note that this definition applies to general sets, not only to finite ones. An infinite set (but not a finite one) can have the same cardinality as a strict subset.

Example: The set of natural numbers $\mathbb{N}$ and the set of even numbers $even := \{2n \mid n \in \mathbb{N}\}$ have the same cardinality, because $f : \mathbb{N} \to even$ with $f(n) = 2n$ is a bijection.

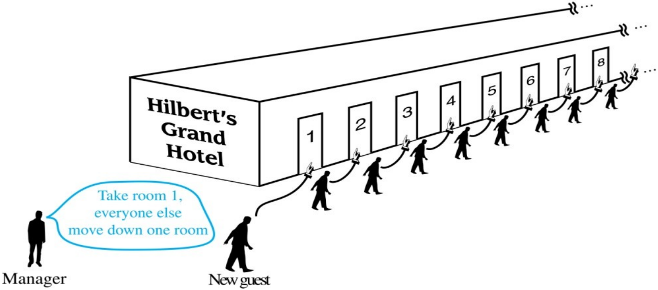
Countable Sets

Definition

- A set S is called **countably infinite**, iff it has the same cardinality as the natural numbers, $|S| = |\mathbb{N}|$.
- A set is called **countable** iff it is either finite or countably infinite.
- A set that is not countable is called **uncountable**.

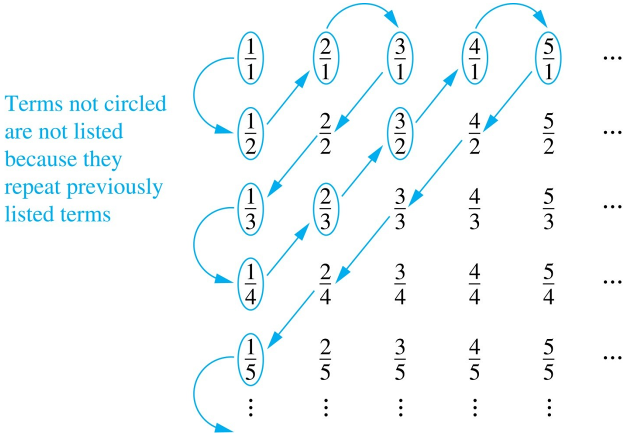
Hilbert's Grand Hotel

The Grand Hotel (example due to David Hilbert) has countably infinite number of rooms, each occupied by a guest. We can always accommodate a new guest at this hotel. How is this possible?



The Positive Rational Numbers are Countable

Construct a bijection $f : \mathbb{N} \rightarrow \mathbb{Q}^+$.
List fractions p/q with $q = n$ in the n-th row.
f traverses this list in the following order.
For $n = 1, 2, 3, \ldots$ **do** visit all p/q with $p + q = n$.



Finite Strings

Theorem

The set Σ^* of all finite strings over a finite alphabet Σ is countably infinite.

Proof.

- First define an (alphabetical) ordering on the symbols in Σ.
- Show that the strings can be listed in a sequence.
  First all strings of length 0 in lexicographic order.
  Then all strings of length 1 in lexicographic order.
  Then all strings of length 2 in lexicographic order, etc.
- This implies a bijection from $\mathbb{N}$ to Σ^*.

$\square$

In particular, the set of all Java-programs is countable, since every program is just a finite string.

Combining Countable Sets

Theorem

The union $S_1 \cup S_2$ of two countably infinite sets S_1, S_2 is countably infinite.

Proof.

(Sketch) Since S_1, S_2 are countably infinite, there must exist bijections $f_1 : \mathbb{N} \to S_1$ and $f_2 : \mathbb{N} \to S_2$. Consider the disjoint parts S_1 and $S_2 - S_1$. If $S_2 - S_1$ is finite then consider this part separately and build a bijection $f : \mathbb{N} \to S_1 \cup S_2$ by shifting f_1 by $|S_2 - S_1|$. Otherwise, construct bijections between the two parts and the even/odd natural numbers, respectively. $\square$

Uncountable Sets

Theorem

The set of infinite binary strings is uncountable.

Proof.

Assume by contraposition that a bijection $f : \mathbb{N} \to \mathit{InfiniteStrings}$ exists. Let d_n be the n-th symbol of string $f(n)$. We define a string x such that the n-th symbol of x is $d_n + 1 \mod 2$. Thus $\forall n \in \mathbb{N}\ x \neq f(n)$ and f is not a surjection. Contradiction. □

Similarly for the infinite decimal strings (over digits $\{0, 1, 2, \ldots, 9\}$). Just use modulo 10 instead of modulo 2.

The technique used in the proof above is called diagonalization.

The Real Numbers are Uncountable

A similar diagonalization argument shows uncountability of $\mathbb{R}$.

Theorem

The real numbers in the interval $(0,1) \subseteq \mathbb{R}$ *are uncountable.*

Proof.

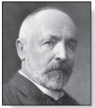
(Sketch) Construct a bijection between $(0,1)$ and the set of infinite binary strings. E.g., a string $10011\ldots$ means the number $0.10011\ldots$. Some slight problem arises because the same number can be represented by different infinite strings. Also infinite strings can be eventually constant. Handle these cases separately. $\square$

Theorem

The real numbers $\mathbb{R}$ *are uncountable.*

Proof.

Find a bijection between $(0,1)$ and $\mathbb{R}$. E.g., $f(x) = \tan(\pi x - \pi/2)$. $\square$

Cantor's Theorem  (Georg Cantor, 1845-1918)

Theorem

Let S be a set and 2^S be its powerset (the set of all subsets of S). There does **not exist** *any surjection $f : S \to 2^S$.*

Proof.

Assume, by contraposition, that such a surjection f exists. We define the set $G \subseteq S$ as follows. $G := \{x \in S \mid x \notin f(x)\}$. Since f is a surjection, there must exist an $s \in S$ s.t. $G = f(s)$. Now there are two cases:

1. If $s \in G$ then, by def. of G, $s \notin f(s) = G$. Contradiction.
2. If $s \notin G = f(s)$ then $s \notin f(s)$. Thus, by def. of G, $s \in G$. Contradiction.

$\square$

Implications of Cantor's Theorem

- By Cantor's Theorem there cannot exist any bijection $f : S \to 2^S$.
- However, an **injection** is trivial to find. Let $f(x) := \{x\}$.
- By the definition of Cardinality this means that $|S| < |2^S|$, i.e., a powerset has strictly larger cardinality than its base set.
- Thus $2^{\mathbb{N}}$ is not countable. (It can also be shown that $|\mathbb{R}| = |2^{\mathbb{N}}|$.)
- The Continuum hypothesis claims there there does not exist any set S with $|\mathbb{N}| < |S| < |\mathbb{R}|$, i.e., nothing strictly between. This problem was 1st on the list of Hilbert's 23 problems presented in 1900. It was shown to be independent of ZFC (Zermelo-Fraenkel set theory) by Gödel/Cohen in 1963, i.e., it cannot be (dis)proven in ZFC.
- There exists an infinite hierarchy of sets of ever larger cardinality. Let $S_0 := \mathbb{N}$ and $S_{i+1} := 2^{S_i}$. Then $|S_i| < |S_{i+1}|$ for all i.
- The existence of even larger cardinals beyond his hierarchy is a problem of axiomatics beyond ZFC. See "Large Cardinals".