L04: Sets and Functions

- **Sets**
- Functions
- Cardinality of Sets

- Reading: Rosen 2.1, 2.2, 2.3, 2.5

Set

- **Definition:** A **set** is an unordered collection of objects The objects in a set are called the **elements** or **members** of the set. A set is said to contain its elements. We write a $a \in A$ to denote that a is an element of the set A and $a \notin A$ to denote that a is not an elements of A.
- **Roster method:**
  - List all elements of a set explicitly
  - Use … when the pattern is obvious.
- **Example**
  - The set of all odd positive integers less than 10 can be denoted by $\{1, 3, 5, 7, 9\}$.
  - The set of all odd positive integers less than 100 can be denoted by $\{1, 3, 5, \ldots, 99\}$.

Set Builder

- We can also use the **set builder** notation to express the set as
  $\{x \mid x \text{ is an odd positive interger less than } 100\}$, or
  $\{x \in \mathbf{Z}^+ \mid x \text{ is odd and } x < 100\}$,
- Generally, we can define a set as $\{x \in E \mid P(x)\}$ or $\{x \in E : P(x)\}$ using a predicate $P(x)$, which contains all $x \in E$ such that $P(x) = T$.
- Remark: Omitting the domain restriction $x \in E$ may lead to paradoxes
  - Russel's paradox: Let $A = \{x \mid x \notin x\}$, then $A \in A$?
  - Leads to axiomatic set theory

Some Important Sets

$\mathbf{N}$ = *natural numbers* = $\{0, 1, 2, 3, \dots\}$

$\mathbf{Z}$ = *integers* = $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

$\mathbf{Z}^+$ = *positive integers* = $\{1, 2, 3, \dots\}$

$\mathbf{Z}^-$ = *negative integers* = $\{-1, -2, -3, \dots\}$

$\mathbf{R}$ = *real numbers*

$\mathbf{R}^+$= *positive real numbers*

$\mathbf{R}^-$= *negative real numbers*

$\mathbf{Q}$ = *rational numbers*

Empty Set and Singleton Set

- **Definition**
  The **empty set** or **null set**, denoted by ∅ or {}, is a special set containing no elements.
- **Definition**
  A set with one element is called a **singleton set**.
- **Example**
  Note that $\emptyset \neq \{\emptyset\}$. The latter is a singleton set.
  Yes, an element of a set can also be a set!
- In pure set theory, everything is a set!

Set Equality

- **Definition**
  Two sets A and B are **equal**, denoted by $A = B$, if and only if they have the same elements, i.e., for every x, $x \in A$ if and only if $x \in B$.
- **Example 3**

$$\{1, 2, 3\} = \{3, 1, 2\} = \{1, 2, 2, 2, 3, 3\}$$

Subset

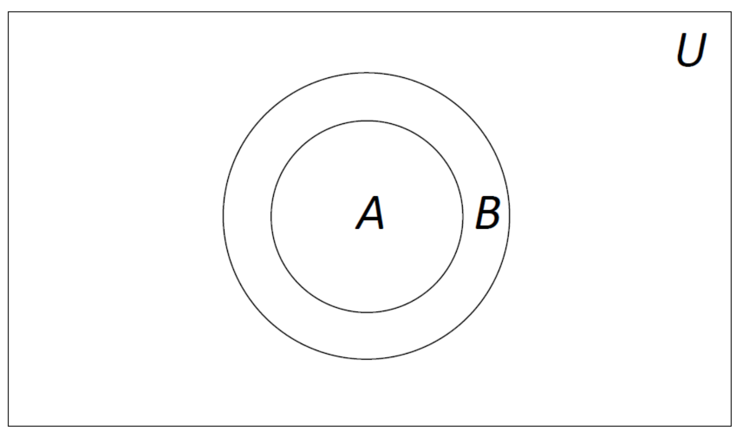
- **Definition**
  A set A is said to be a **subset** of a set B, denoted by $A \subseteq B$, if and only if every element of A is also an element of B.
- **Note**
  For every set S, (a) $\emptyset \subseteq S$ and (b) $S \subseteq S$.
- **Remark**
  Every nonempty set is guaranteed to have at least two subsets, the empty set and the set itself.
- $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

Proper Subset

- **Definition**

  A set A is said to be a **proper subset** of a set B, denoted by $A \subset B$, if and only if $A \subseteq B$ but $A \neq B$.

We can use a **Venn diagram** to illustrate, among other things, the subset relationship.



Cardinality of Finite Sets

- **Definition**
  Let S be a finite set. The cardinality of S, denoted by $|S|$, is the number of (distinct) elements in S.
- **Definition**
  A set is said to be infinite if it is not finite.

Power Set

- **Definition**
  Given a set S, the power set of S, denoted by $P(S)$, is the set of all subsets of S.
- **Remark**
  If a set has n elements where n is a nonnegative integer, then its power set has 2^n elements.
- **Example**
  The power set of the set $\{a, b, c\}$ is $P(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.
- **Example**
  What is the power set of the empty set? What is the power set of the set $\{\emptyset\}$?

Ordered Tuple

- **Definition**
  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, …, and $\boldsymbol{a_n}$ as its n-th element. An ordered 2-tuple is more commonly called an **ordered pair**.
- **Definition**
  Two ordered n-tuples $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ are equal if and only if $m = n$ and $a_i = b_i$ for all $i = 1,2, \ldots, n$.

Cartesian Product

- **Definition**

  Let A and B be two 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 $b \in B$, i.e.

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}.$$

- **Example**

  Let $A = \{1,2\}$ and $B = \{a, b, c\}$. The Cartesian product is

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

Relation

- **Definition**

  Let A and B be two sets. A subset R of $A \times B$ is called a **relation** from the set A to be the set B.

- **Example**

  Let $A = \{1,2\}$ and $B = \{a, b, c\}$. The Cartesian product is

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

and $R = \{(1, a), (1, c), (2, a), (2, b)\} \subset A \times B$ is a relation from A to B.

Cartesian Product

- **Definition**

  The **Cartesian product** of the sets A_1, A_2, …, A_n denoted by $A_1 \times A_2 \times \cdots \times A_n$, is the set of ordered *n*-tuples $(a_1, a_2, \ldots, a_n)$, where a_i belongs to A_i for $i = 1,2, \ldots, n$, i.e.

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ for } i = 1,2, \ldots, n\}.$$

Union

- **Definition**

  Let A and B be two sets. The **union** of 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.

- **Definition**

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

Intersection

- **Definition**

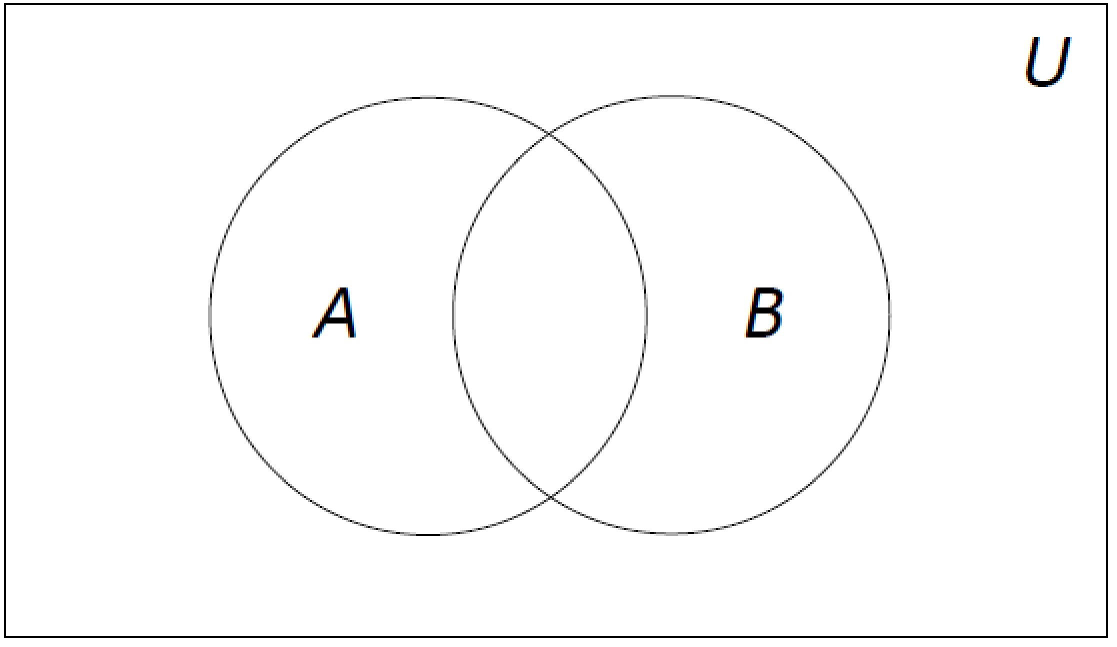
  Let A and B be two sets. The **intersection** of A and B, denoted by $A \cap B$, is the set that contains those elements that are in both A and B.
- **Definition**

  Let $A_1, A_2, \dots, A_n$ be *n* sets. The **intersection** of the collection of *n* sets, denoted by $\cap_{i=1}^{n} A_i$, is the set that contains those elements that are members of all the sets in the collection.
- **Definition**

  Two sets A and B are **disjoint** iff $A \cap B = \emptyset$.

Union, Intersection, and Cardinality

- **Theorem**
  Let A and B be two finite sets. The cardinality of their union $|A \cup B| = |A| + |B| - |A \cap B|$.



Difference and Complement

- **Definition**

  Let A and B be two sets. The **difference** of A and B, denoted by $A - B$ or $A \backslash B$, is the set containing those elements that are in A but not in B. It is also called the **complement of B with respect to A**

- **Example**

  $\{1,3,5\} - \{1,2,3\} = \{5\}$.

- **Definition**

  Let U be the universal set. The **complement** of a Set A, denoted by $\bar{A}$, is the complement of A with respect to U. In other words, it is $U - A$.

Set Identities

Set identities	
Identity	Name
$A \cup \emptyset = A$ $A \cap U = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws

Set Identities (cont'd)

Set identities	
Identity	Name
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive laws
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

Set Identities and Logic Equivalences

- All these set identities follow from corresponding logic equivalences
- Example: De Morgan's law

$$
\begin{aligned}
\overline{A \cap B} &= \{x | x \notin A \cap B\} && \text{by defn. of complement} \\
&= \{x | \neg(x \in (A \cap B))\} && \text{by defn. of does not belong symbol} \\
&= \{x | \neg(x \in A \wedge x \in B\} && \text{by defn. of intersection} \\
&= \{x | \neg(x \in A) \vee \neg(x \in B)\} && \text{by 1st De Morgan law} \\
& && \text{for Prop Logic} \\
&= \{x | x \notin A \vee x \notin B\} && \text{by defn. of not belong symbol} \\
&= \{x | x \in \overline{A} \vee x \in \overline{B}\} && \text{by defn. of complement} \\
&= \{x | x \in \overline{A} \cup \overline{B}\} && \text{by defn. of union} \\
&= \overline{A} \cup \overline{B} && \text{by meaning of notation}
\end{aligned}
$$

- So, just replace $\cap$ with $\wedge$, $\cup$ with $\vee$, $\overline{\ \ }$ with $\neg$

Outline

- Sets
- **Functions**
- Cardinality of Sets

Function

- **Definition:** Let A and B be nonempty sets. A **function** from A to B is an assignment of exactly one element of B to each element of A. We write $f(a) = b$, if b is the unique element of B assigned by the function f to the element a of A. If f is a function from A to B, we write $f: A \to B$.
- **Remark:** Functions are sometime also called **mappings** or **transformations**. If f is a function from A to B, we say that f **maps** A to B.
- **Definition:** If f is a function from A to B, we say that A is the **domain** of f and B is the **codomain** of f. If $f(a) = b$, we say that b is the **image** of a and a is the **preimage** of b. The **range** of f is the set of all images of elements of A.

Examples

- **Example 8**

  Let f be the function that assigns the last two bits of a bit string of length 2 or greater to that string. For example, $f(11010) = 10$. Then, the domain of f is the set of all bit string of length 2 or greater, and both the codomain and range are the set $\{00, 01, 10, 11\}$.
- **Example 9**

  Let $f: \mathbf{Z} \to \mathbf{Z}$ assign the square of an integer to this integer. Then $f(x) = x^2$, where the domain of f is the set of all integers, we take the codomain of f to be the set of all integers, and the range of f is the set of all integers that are perfect squares, namely, $\{0, 1, 4, 9, \ldots\}$.

Injective Function

- **Definition**

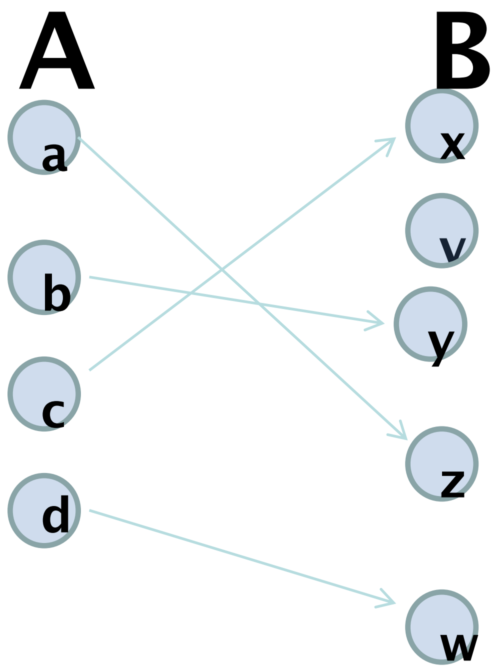
  A function f is said to be **injective** (or **one-to-one**) if and only if $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f. An injective function is also called an **injection**.

- **Example**

  Is the function $f(x) = x + 1$ from the set of real numbers to the set of real numbers injective?

- **Example**

  Is the function $f(x) = x^2$ from the set of integers to the set of integers injective?



Surjective Function

- **Definition**

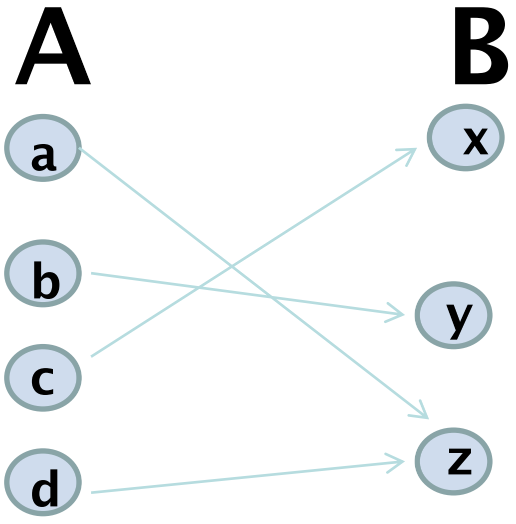
  A function f from set A to the set B is said to be **surjective** (or **onto**) if and only if every element $b \in B$ there is an element $a \in A$ with $f(a) = b$. A surjective function is also called a **surjection**.

- **Example**

  Is the function $f(x) = x + 1$ from the set of integers to the set of integers surjective?

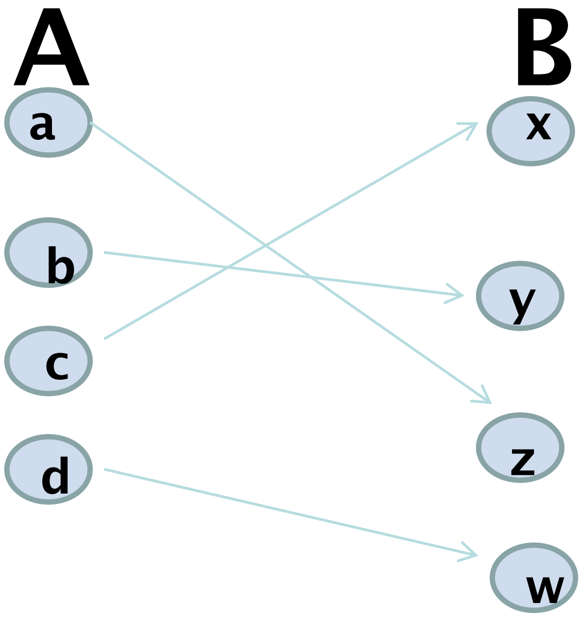
- **Example**

  Is the function $f(x) = x^2$ from the set of integers to the set of integers surjective?



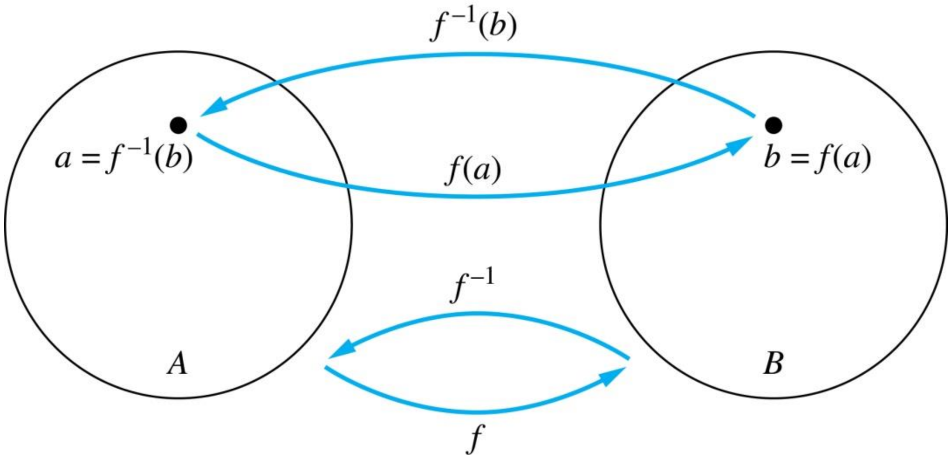
Bijection

- **Definition**
  A function f is a **bijection** (or **one-to-one correspondence**) if it is both one-to-one and onto.
- Note: By convention, the "if" immediately following a definition means "iff".
- Note:
  - one-to-one: injection
  - one-to-one correspondence: bijection



Inverse Function

- **Definition** Let f be a one-to-one correspondence from the set A to the set B. The **inverse function** of f is the function that assigns to an element b belonging to B the unique element a in A such that $f(a) = b$. The inverse function of f is denoted by f^{-1}. Hence, $f^{-1}(b) = a$ when $f(a) = b$.
- A one-to-one correspondence is called **invertible**.

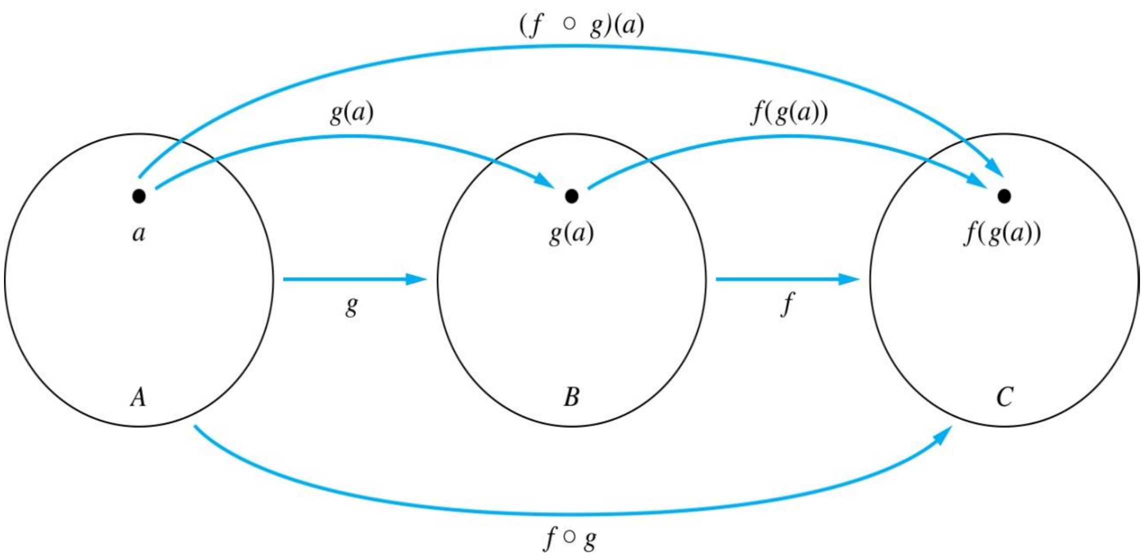


Examples

- **Example**
  Let $f: \mathbf{Z} \to \mathbf{Z}$ be such that $f(x) = x + 1$. Is f invertible, and if it is, what is its inverse?
- **Example**
  Let $f: \mathbf{R} \to \mathbf{R}$ be such that $f(x) = x^2$. Is f invertible?

Composition

- **Definition**
  Let g be a function from the set A to the set B and let f be a function from the set B to the set C. The **composition** of the functions f and g, denoted by $f \circ g$, is defined by $(f \circ g)(a) = f\big(g(a)\big)$.



Composition

- **Example**

  Let f and g be functions from $\mathbf{Z}$ to $\mathbf{Z}$ defined by $f(x) = 2x + 3$ and $g(x) = 3x + 2$. What is the composition of f and g? What is the composition of g and f?

Outline

- Sets
- Functions
- **Cardinality of Sets**

Hilbert's Grand Hotel

- Suppose a hotel has infinitely many rooms, numbered 1, 2, 3, …
- All rooms are occupied
- A new guest arrives…
- It means $|\{1, 2, \ldots,\}| = |\{2, 3, \ldots\}|$
- https://www.youtube.com/watch?v=OxGsU8oIWjY

Cardinality of Infinite Sets

- **Definition:** Two sets A and B have the same cardinality if and only if there is a one-to-one correspondence from A to B.
- **Definition:**
  $$|\mathbf{N}| = \aleph_0$$
  where $\mathbf{N}$ is the set of natural numbers {0, 1, 2, …}
- A set S is
  - finite, if $|S| = n$ for some $n \in \mathbf{N}$
  - infinitely countable if $|S| = \aleph_0$
  - otherwise, uncountable

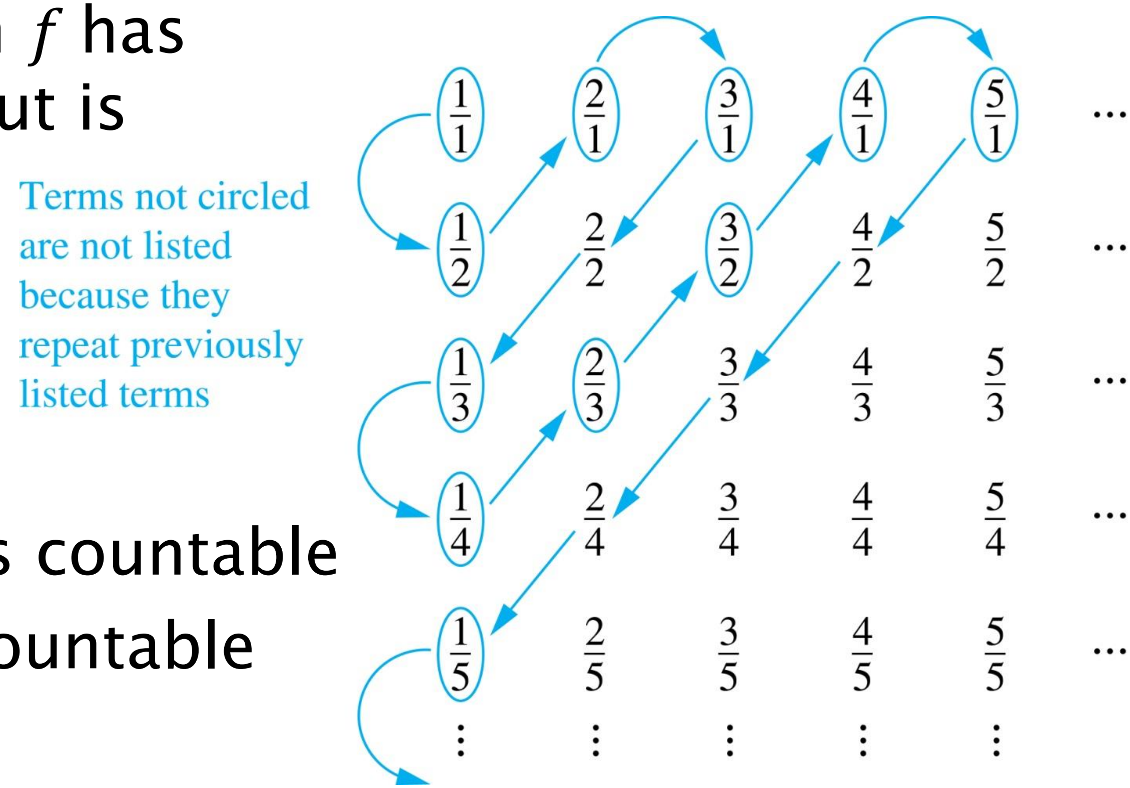
countable

Examples

- **Example:**
  $\mathbf{Z}^+ = \{1, 2, 3, \ldots\}$ is countable.
  Let $f: \mathbf{N} \rightarrow \mathbf{Z}^+$ be $f(x) = x + 1$
- **Example:**
  The set of all nonnegative even numbers is countable.
  $$f(x) = 2x$$
- **Example:**
  The set of all integers $\mathbf{Z}$ is countable.
- Solution:
  List all integers as: $0, 1, -1, 2, -2, 3, -3, \ldots$
  Define $f(x) = \begin{cases} -\frac{x}{2}, if\ x\ is\ even \\ \frac{x+1}{2}, if\ x\ is\ odd \end{cases}$

$\mathbf{Q}$ is countable

- Will only show that $\mathbf{Q}^+$ is countable
- Recall: A *rational number* can be expressed as the ratio of two integers p and q such that $q \neq 0$.
- Note: the function f has no closed form, but is well defined.

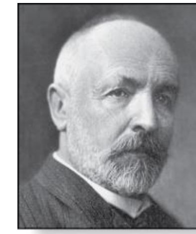


- **Corollary**: $\mathbf{N} \times \mathbf{N}$ is countable
- **Corollary**: $\mathbf{N}^k$ is countable for any $k \in \mathbf{Z}^+$.

Strings

- Fix an alphabet Σ
  - E.g., $\Sigma = \{a, b, \dots z\}$ for English words
  - $\Sigma = \{0, 1\}$ for machine code of computer programs
- **Theorem**: The set of strings over Σ is countable
- Proof (using $\Sigma = \{0, 1\}$ as example):
  - Strings of length 0: empty string
  - Strings of length 1: $0, 1$
  - Strings of length 2 in lexicographical order: $00, 01, 10, 11$
  - Strings of length 3 in lexicographical order: $000, 001, 010, 011, 100, 101, 110, 111$
  - …

$\mathbf{R}$ is uncountable



Georg Cantor
(1845-1918)

- **Theorem**: $(0,1)$ is uncountable
- Proof by contradiction:
  - Suppose it is countable, then the real numbers in $(0,1)$ can be listed as

$$\begin{aligned} r_1 &= 0.d_{11}d_{12}d_{13}d_{14}d_{15}d_{16}\ldots \\ r_2 &= 0.d_{21}d_{22}d_{23}d_{24}d_{25}d_{26}\ldots \\ r_3 &= 0.d_{31}d_{32}d_{33}d_{34}d_{35}d_{36}\ldots \\ &\vdots \end{aligned}$$

Technical note: A real number may have two decimal representations: $1 = 0.\dot{9}$, $0.353 = 0.352\dot{9}$. We choose the former one.

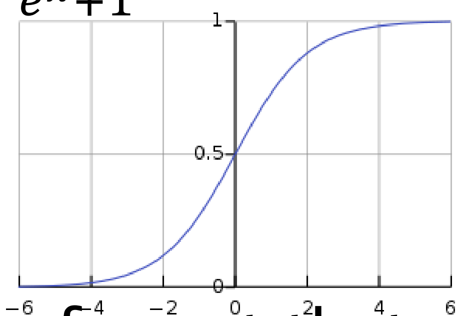
- Form a new real number $r = 0.d_1d_2\ldots$, where

$$d_i = \begin{cases} 4, \text{if } d_{ii} \neq 4, \\ 5, \text{if } d_{ii} = 4. \end{cases}$$

- Key observation: $r \neq r_i$ for any i!
- So, r is not in the list, a contradiction.
- A diagonalization argument

Compare infinite sets

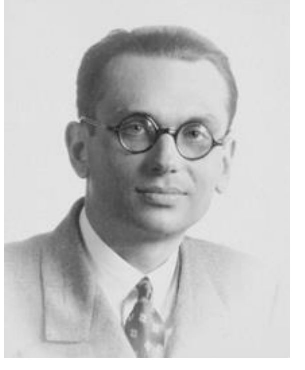
- We write $|S| \leq |T|$, if there is an injection from S to T. We write $|S| < |T|$, if there exists an injection but no bijection from S to T.
- We have shown that there is no bijection from $\mathbf{N}$ to $(0, 1)$
- Find an injection from $\mathbf{N}$ to $(0, 1)$: $f(x) = \frac{e^x}{e^x+1}$

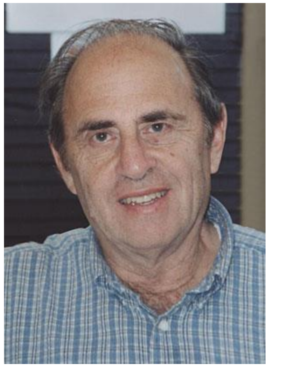


- So $|\mathbf{N}| < |(0, 1)| = |\mathbf{R}|$
  - What's a bijection between $(0, 1)$ and $\mathbf{R}$?
- **Corollary**: There is no computer number format that can represent all real numbers.

The Continuum Hypothesis

- There is no set whose cardinality is strictly between that of natural numbers and that of real numbers (Hilbert's first problem, 1900).
- Cannot be proved or disproved in ZFC (an axiomatic set theory)
  - Kurt Gödel, 1940
  - Paul Cohen, 1963





Schröder-Bernstein Theorem

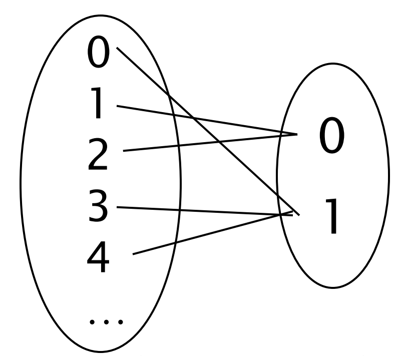
- **Theorem:** If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.
- No easy proof for this seemingly obvious fact!
- **Example:** Show that $|(0,1)| = |(0,1]|$.
- Proof:
  - An injection $(0,1) \to (0,1]$: $f(x) = x$
  - An injection $(0,1] \to (0,1)$: $f(x) = \frac{x}{2}$

$|S| < |P(S)|$

- **Theorem:** For any set S, $|S| < |P(S)|$
- Proof:
- An injection $S \to P(S)$: $f(a) = \{a\}$
- Difficult part is to show that there is no bijection
- Let g be any function from S to $P(S)$. Will show that g is not surjective, hence not bijective.
- Consider $A = \{x \in S \mid x \notin g(x)\}$. Note $A \subseteq S$, so $A \in P(S)$
- Will show that for no $a \in S$, $g(a) = A$.
- Suppose for some $a \in S$, $g(a) = A$, then
- $a \in A \Leftrightarrow a \in \{x \in S \mid x \notin g(x)\}$
  $\Leftrightarrow a \notin g(a) \Leftrightarrow a \notin A$, a contradiction.
- **Corollary:** $P(\mathbf{N})$ is uncountable.

Uncomputable functions

- Definition: A function is computable if there is a computer program that finds the value of the function on any input, otherwise it is uncomputable.
- **Theorem**: There exist functions from $\mathbf{N}$ to $\{0,1\}$ that are uncomputable.
- Proof:
- |The set of computer programs| = $|\mathbf{N}|$, countable
- |The set of functions $\mathbf{N} \to \{0,1\}$| = $|P(\mathbf{N})|$, uncountable
  - Every function $g: \mathbf{N} \to \{0,1\}$ maps to a $S \subseteq \mathbf{N}$
  - $S = \{x \in \mathbf{N} \mid g(x) = 1\}$
- A concrete uncomputable function: The halting problem.



S={0, 3, 4,…}

Alan Turing