03 Sets and Functions

CS201 Discrete Mathematics

Instructor: Shan Chen

Russell's Paradox

- Let $S = \{ x \mid x \notin x \}$ be a set of sets that are not members of themselves.

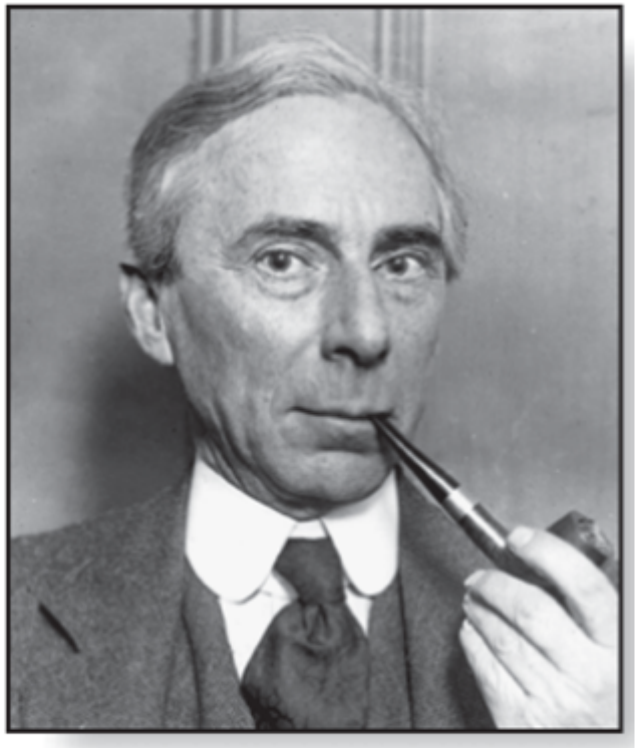
- Paradox:
  - If P is a property, then the set $\{ x \mid P(x) \}$ exists (naive set theory): S must exist
  - $S \in S$?

    S does not satisfy the property, so $S \notin S$.
  - $S \notin S$?

    S is included in the set S, so $S \in S$.
  - $S \in S \leftrightarrow S \notin S$: S does not exist

- **Solution:** axiomatic set theory (e.g., **Zermelo–Fraenkel**)

  ** out of scope of this course*



Bertrand Russell (1872-1970)
Cambridge, UK
Nobel Prize Winner

Sets

Sets

- A set is an unordered collection of objects. These objects are called elements or members.

- Two sets A, B are equal if and only if $\forall x\ (x \in A \leftrightarrow x \in B)$.

- Many discrete structures are built with sets:
  - Combinations (counting)
  - Relations
  - Graphs
  - …

Sets

- A set is an unordered collection of objects. These objects are called elements or members.

- Examples:
  - $S = \{2, 3, 5, 7\}$
  - $A = \{1, 2, 3, \ldots, 100\}$
  - $B = \{a \geq 2 \mid a \text{ is a prime}\}$
  - $C = \{2n \mid n = 0, 1, 2, \ldots\}$

- Different ways to represent a set:
  - Listing (enumerating) the elements
  - Using ellipses "…" if enumeration is hard
  - Set builder: $\{ x \mid x \text{ has property } P \}$ or $\{ x \mid P(x) \}$

Important Sets

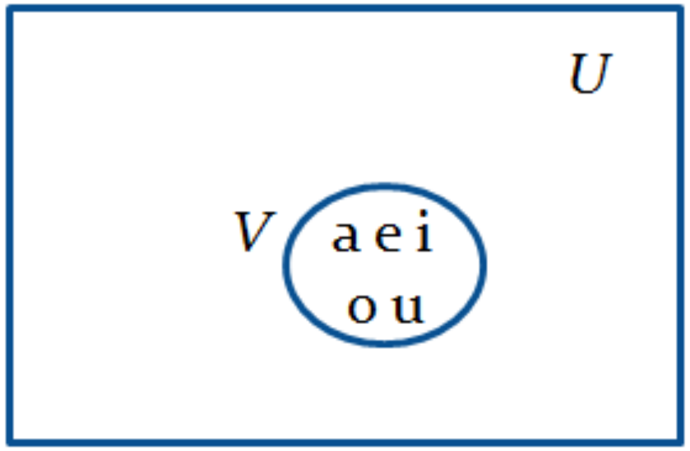
- Natural numbers: $\boldsymbol{N} = \{\ 0, 1, 2, 3, \ldots\ \}$
- Integers: $\boldsymbol{Z} = \{\ \ldots, -2, -1, 0, 1, 2, \ldots\ \}$
- Positive integers: $\boldsymbol{Z}^+ = \{\ 1, 2, 3, \ldots\ \}$
- Rational numbers: $\boldsymbol{Q} = \{\ p/q \mid p, q \in \boldsymbol{Z}, q \neq 0\ \}$
- Real numbers: $\boldsymbol{R}$
- Complex numbers: $\boldsymbol{C} = \{\ a + bi \mid a, b \in \boldsymbol{R}\ \}$

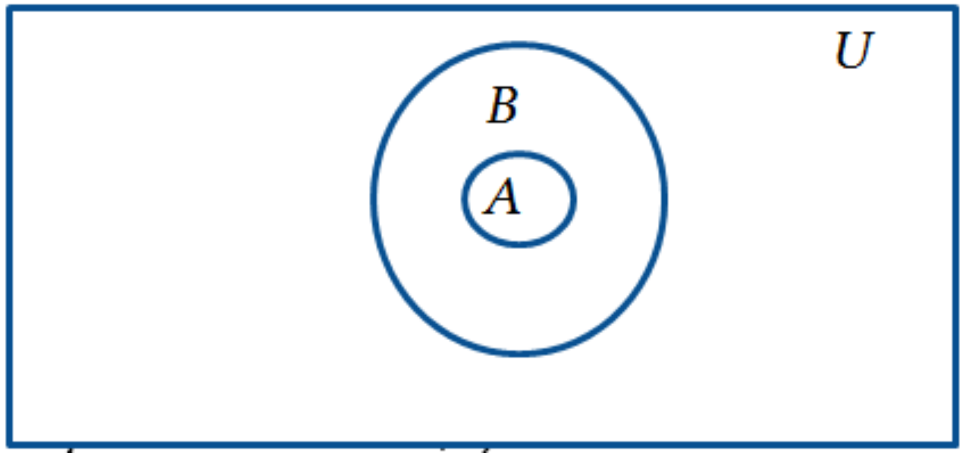
Interval Notation

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

Special Sets and Venn Diagrams

- **Universal set:** the set of all objects under consideration, denoted by U.
- **Empty set:** the set of no object, denoted by $\varnothing$ or $\{\}$.
  - Note that $\varnothing \neq \{\varnothing\}$
- Sets can be visualized using **Venn diagrams**.





John Venn (1834-1923)
Cambridge, UK

Subsets and Proper Subsets

- A set A is called a subset of B, denoted by $A \subseteq B$, if and only if every element of A is also an element of B: $\forall x\, (x \in A \rightarrow x \in B)$

- If $A \subseteq B$ but $A \neq B$, then we say A is a proper subset of B, denoted by $A \subset B$, i.e., $\forall x\, (x \in A \rightarrow x \in B) \wedge \exists x\, (x \in B \wedge x \notin A)$

- Two sets are equal if and only if each is a subset of the other

$$A = B \quad \text{if and only if} \quad A \subseteq B \text{ and } B \subseteq A$$

$$\forall x\, (x \in A \leftrightarrow x \in B) \leftrightarrow (\forall x\, (x \in A \rightarrow x \in B) \wedge \forall x\, (x \in B \rightarrow x \in A))$$

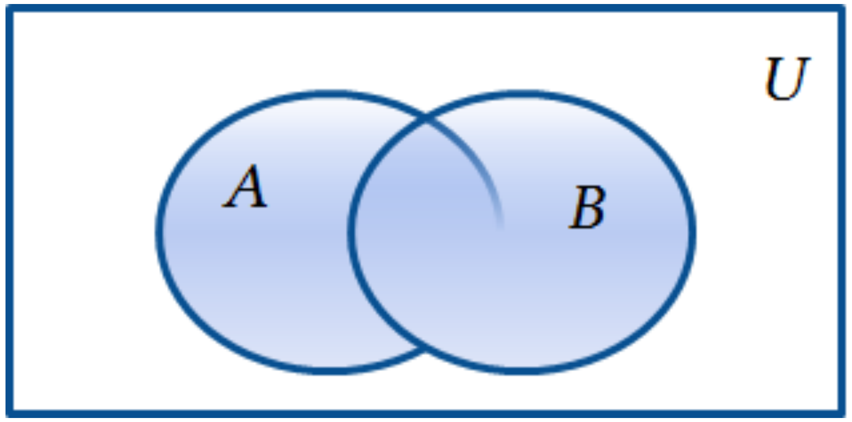
Subset Properties

- **Theorem:** $\varnothing \subseteq S$
- Proof: By definition, we need to prove $\forall x(x \in \varnothing \rightarrow x \in S)$.
  Since $\varnothing$ does not contain any element, $x \in \varnothing$ is always false.
  Then the implication is always true. * *vacuous proof*
- **Theorem:** $S \subseteq S$
- Proof: By definition, we need to prove $\forall x(x \in S \rightarrow x \in S)$, which is obviously true.

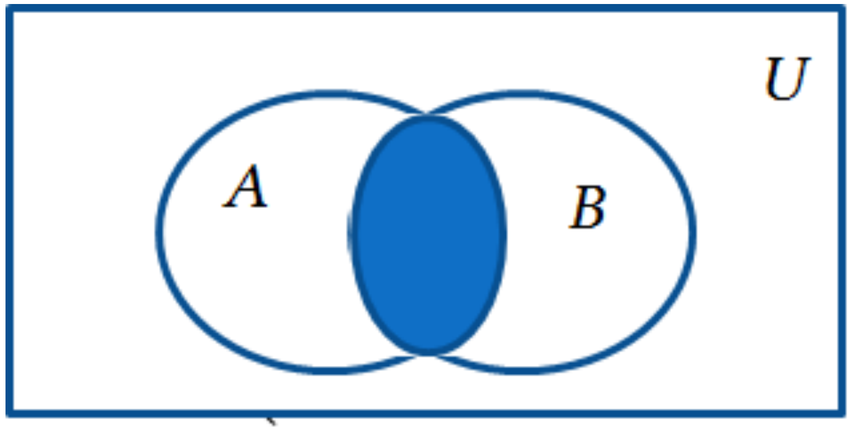
SUSTech

Set Operations

- **Union:** The union of sets A and B, denoted by $A \cup B$, is the set $\{ x \mid x \in A \vee x \in B \}$.

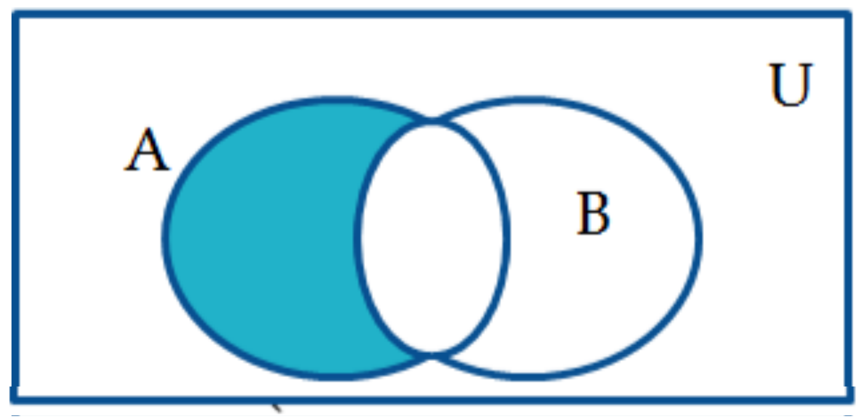


- **Intersection:** The intersection of sets A and B, denoted by $A \cap B$, is the set $\{ x \mid x \in A \wedge x \in B \}$. Two sets A and B are called disjoint if their intersection is empty, i.e., $A \cap B = \varnothing$.

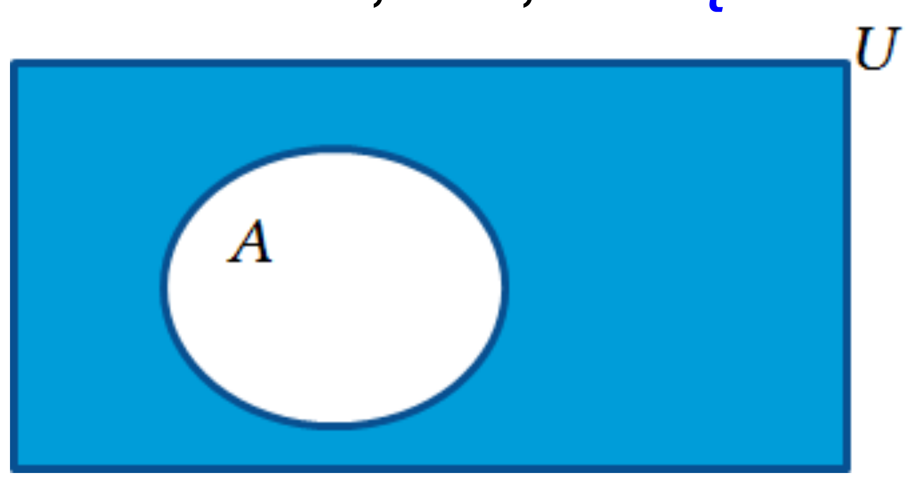


Set Operations

- **Difference:** The difference of sets A and B, denoted by $A - B$, is the set that contains all the elements of A that are not in B, i.e., $A - B = \{ x \mid x \in A \wedge x \notin B \}$.



- **Complement:** The complement of set A (w.r.t. universal set U), denoted by $\bar{A}$ is the set $U - A$, i.e., $\bar{A} = \{ x \in U \mid x \notin A \}$.



Exercise *(1 min)*

- Let $U = \{ 0, 1, \ldots, 10 \}$, $A = \{ 1, 2, 3, 4, 5 \}$, $B = \{ 4, 5, 6, 7, 8 \}$. Compute the following:
- $A \cup B$
- $A \cap B$
- $\bar{A}$
- $\bar{B}$
- $A - B$
- $B - A$

Exercise *(1 min)*

- Let $U = \{ 0, 1, \ldots, 10 \}$, $A = \{ 1, 2, 3, 4, 5 \}$, $B = \{ 4, 5, 6, 7, 8 \}$. Compute the following:
- $A \cup B$ $\{1, 2, \ldots, 8\}$
- $A \cap B$ $\{4, 5\}$
- $\bar{A}$ $\{0, 6, 7, 8, 9, 10\}$
- $\bar{B}$ $\{0, 1, 2, 3, 9, 10\}$
- $A - B$ $\{1, 2, 3\}$
- $B - A$ $\{6, 7, 8\}$

SUSTech

Union and Intersection (Generalized)

- **The union of a collection of sets:** the set that contains those elements that are members of at least one set in the collection: $\cup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$.

- **The intersection of a collection of sets:** the set that contains those elements that are members of all sets in the collection: $\cap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$.

Set Identities

- Identity laws
  - $A \cup \varnothing = A$
  - $A \cap U = A$
- Domination laws
  - $A \cup U = U$
  - $A \cap \varnothing = \varnothing$
- Idempotent laws
  - $A \cup A = A$
  - $A \cap A = A$
- Commutative laws
  - $A \cup B = B \cup A$
  - $A \cap B = B \cap A$
- Associative laws
  - $A \cup (B \cup C) = (A \cup B) \cup C$
  - $A \cap (B \cap C) = (A \cap B) \cap C$
- Distributive laws
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Set Identities

- Absorption laws
  - $A \cup (A \cap B) = A$
  - $A \cap (A \cup B) = A$
- Complement laws
  - $A \cup \bar{A} = U$
  - $A \cap \bar{A} = \emptyset$
- De Morgan's laws
  - $\overline{A \cap B} = \bar{A} \cup \bar{B}$
  - $\overline{A \cup B} = \bar{A} \cap \bar{B}$
- Complementation laws
  - $\bar{\bar{A}} = A$

How do we prove these laws?

Let's see the first De Morgan's law for example…

Proofs of $\overline{A \cap B} = \bar{A} \cup \bar{B}$

- Using membership tables: ** requires tedious calculations*

A	B	$\overline{A}$	$\overline{B}$	$\overline{A \cap B}$	$\overline{A} \cup \overline{B}$
1	1	0	0	0	0
1	0	0	1	1	1
0	1	1	0	1	1
0	0	1	1	1	1

Proofs of $\overline{A \cap B} = \bar{A} \cup \bar{B}$

- Using set builder notation and logical equivalences:

$\overline{A \cap B}$	$= \{ x \mid x \in \overline{A \cap B} \}$	*Definition*
	$= \{ x \mid x \notin A \cap B \}$	*Definition of complement*
	$= \{ x \mid \neg(x \in (A \cap B)) \}$	*Definition*
	$= \{ x \mid \neg(x \in A \wedge x \in B) \}$	*Definition of intersection*
	$= \{ x \mid \neg(x \in A) \vee \neg(x \in B) \}$	*De Morgan's*
	$= \{ x \mid x \notin A \vee x \notin B \}$	*Definition*
	$= \{ x \mid x \in \bar{A} \vee x \in \bar{B}) \}$	*Definition of complement*
	$= \{ x \mid x \in \bar{A} \cup \bar{B} \}$	*Definition of union*
	$= \bar{A} \cup \bar{B}$	*Definition*

- Using logical equivalence without set builders: * *less elegant*
  - Prove $\forall x(x \in \overline{A \cap B} \leftrightarrow x \in \bar{A} \cup \bar{B})$ is a tautology. * *see textbook*

Cardinality

- Let S be a set. If there are exactly n distinct elements in S, where n is a nonnegative integer, we say that S is a finite set and n is the cardinality of S, denoted by $|S|$.

- A set S is infinite if it is not finite.

- Examples:
  - $A = \{ 1, 2, 3, \ldots, 20 \}$ $|A| = 20$
  - $B = \{ 1, 2, 3, \ldots \}$ infinite
  - $\varnothing$ $|\varnothing| = 0$

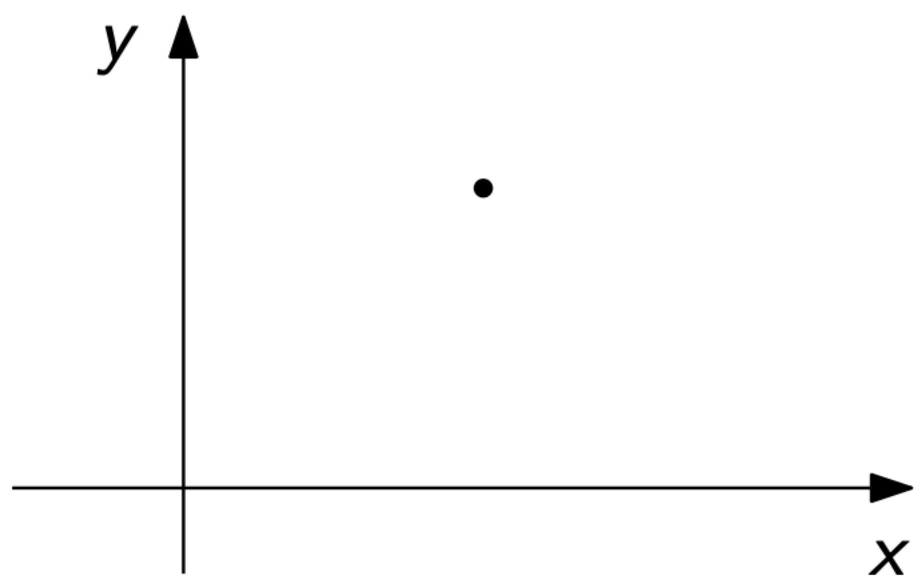
- **Cardinality of the union:** $|A \cup B| = |A| + |B| - |A \cap B|$
  - $|A \cap B|$ counted twice in $|A| + |B|$
  - Known as the inclusion-exclusion principle for 2 sets

SUSTech

Tuples

- An n-tuple $(a_1, a_2, \ldots, a_n)$ is an ordered collection that has a_1 as its first element, a_2 as its second element, and so on, until a_n as its last element.

- Example: coordinates of a point in the 2-D plane are 2-tuples



Cartesian Product

- Let A and B be sets. The Cartesian product of A and B, denoted by $A \times B$, is the set of all 2-tuples (a, b), for $a \in A$ and $b \in B$:

$$A \times B = \{ (a, b) \mid a \in A \land b \in B \}$$

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

- Properties:
  - $A \times B \neq B \times A$ * *order matters*
  - $|A \times B| = |A| \times |B|$ if A, B are finite sets

Cartesian Product (Generalized)

- In general, the Cartesian product of sets $A_1, A_2, \ldots, A_n$, denoted by $A_1 \times A_2 \times \ldots \times A_n$, is defined as:

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

- Example: $A = \{ 0, 1 \}$, $B = \{ 1, 2 \}$, $C = \{ 0, 1, 2 \}$
  - $A \times B \times C = \{ (0,1,0), (0,1,1), (0,1,2), (0,2,0), (0,2,1), (0,2,2), (1,1,0)$ $(1,1,1), (1,1,2), (1,2,0), (1,2,1), (1,2,2) \}$

Power Sets

- Given a set S, the power set of S is the set of all subsets of the set S, denoted by $\mathcal{P}(S)$.

- Examples:
  - $\varnothing$ $\qquad\qquad \mathcal{P}(\varnothing) = \{\varnothing\}$
  - $\{1\}$ $\qquad\qquad \mathcal{P}(\{1\}) = \{\varnothing, \{1\}\}$
  - $\{1, 2\}$ $\qquad\qquad \mathcal{P}(\{1,2\}) = \{\varnothing, \{1\}, \{2\}, \{1,2\}\}$
  - $\{1, 2, 3\}$ $\qquad\qquad \mathcal{P}(\{1,2,3\}) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$

- If S is a set with $|S| = n$, then $|\mathcal{P}(S)| = ?$
  - $|\mathcal{P}(S)| = 2^n$ *Hint: each element is either in the subset or not in it*

Computer Representation of Sets

- **Question:** How to represent sets in a computer?
  - **Naive solution:** explicitly store the elements of a set in a list
  - **Better solution:** (to store many sets w.r.t. the same universal set) assign a bit in a bit string to each element in the universal set and set the bit to *1* if the element is in the set and set it to *0* if otherwise

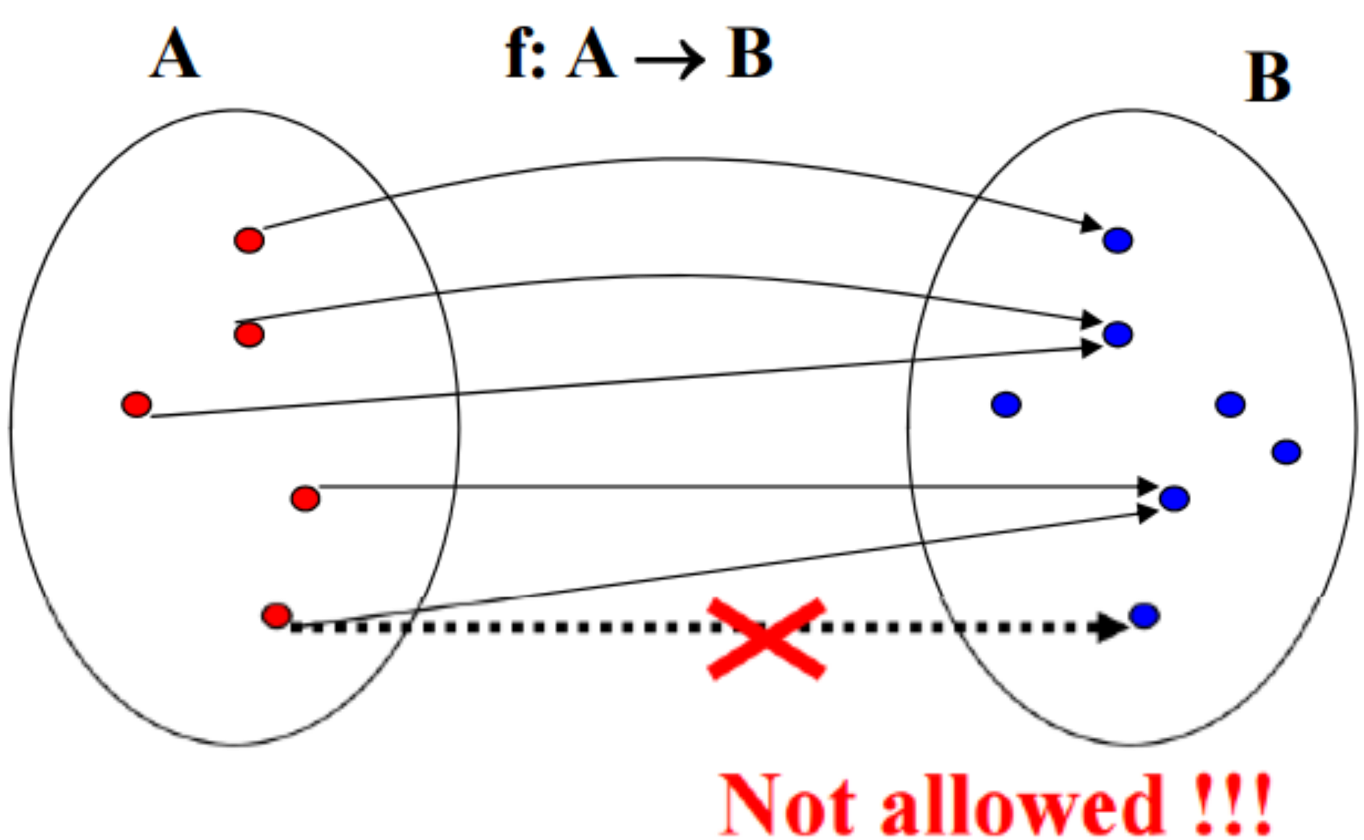
- Example: $U = \{ 1, 2, 3, 4, 5 \}$, $A = \{ 2, 5 \}$, $B = \{ 1, 5 \}$
  - Sets as bit strings: $A = 01001$, $B = 10001$
  - Union: A or $B = 11001 = \{ 1, 2, 5 \}$
  - Intersection: A and $B = 00001 = \{ 5 \}$
  - Complement: A xor $11111 = 10110 = \{ 1, 3, 4 \}$

** set operations converted to bitwise operations of Boolean algebra*

Functions

Functions

- Let A and B be two sets. A function from A to B, denoted by $f : A \to B$, 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.
  - Also called a mapping or transformation.



SUSTech

Representing Functions

- Representing functions $f : A \to B$:
  - explicitly state the assignments between elements from A to B
  - use a formula

- Examples:
  - $A = \{1, 2, 3\}$, $B = \{a, b, c\}$

    f is defined as $1 \mapsto c, 2 \mapsto a, 3 \mapsto c$. Is f a function?

    Yes

    g is defined as $1 \mapsto c, 1 \mapsto b, 2 \mapsto a, 3 \mapsto c$. Is g a function?

    No

  - $A = \{0, 1, \ldots, 9\}$, $B = \{0, 1, 2\}$

    h is defined as $h(x) = x \bmod 3$. Is h a function?

    Yes

Important Sets of Functions

- Let f be a function from A to B. We say that A is the domain of f and B is the codomain of f. If $f(a) = b$, b is called the image of a and a is a preimage of b. The range of f is the set of all images of elements of A, denoted by $f(A)$. We also say f maps A to B.

- Example: $f : \{ 1, 2, 3 \} \to \{ a, b, c \}$ shown in the following figure
    - the image of 1 is c
    - 2 is a preimage of a
    - the domain of f is $\{1, 2, 3\}$
    - the codomain of f is $\{a, b, c\}$
    - the range of f is $\{a, c\}$

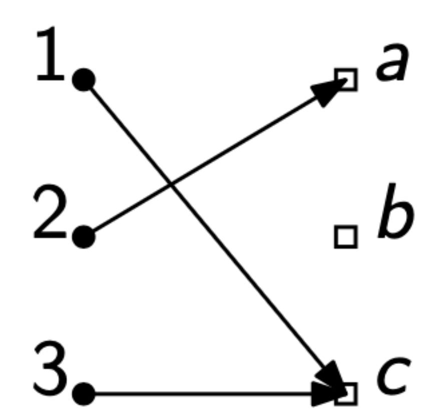
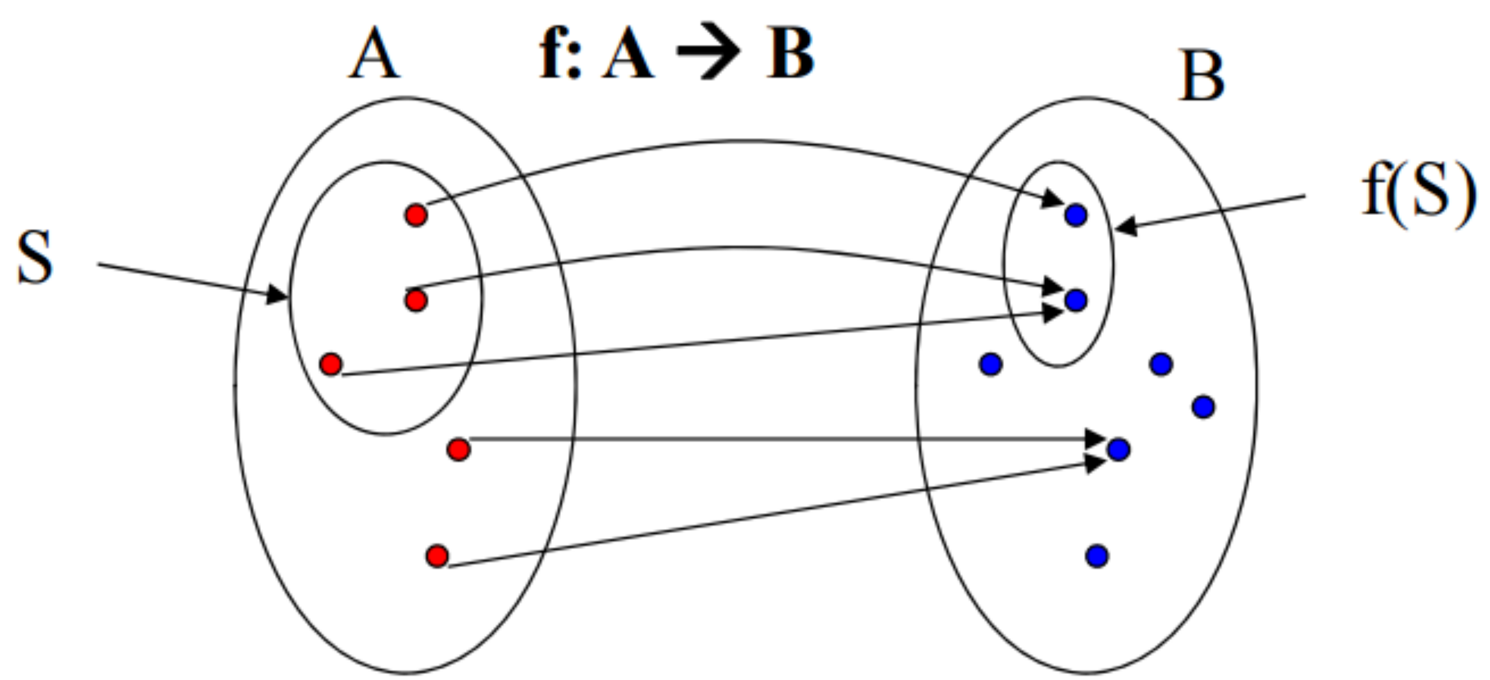
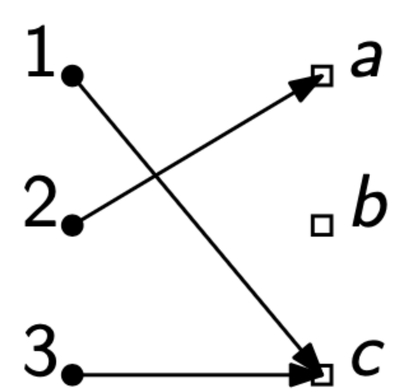


Image of a Subset

- For a function $f : A \rightarrow B$ and $S \subseteq A$, the image of S is a subset of B that consists of the images of elements in S, denoted by $f(S)$, i.e., $f(S) = \{ f(x) \mid x \in S \}$.



- Example: Let $S = \{ 1, 3 \}$, what is $f(S)$?
  - $f(S) = \{c\}$

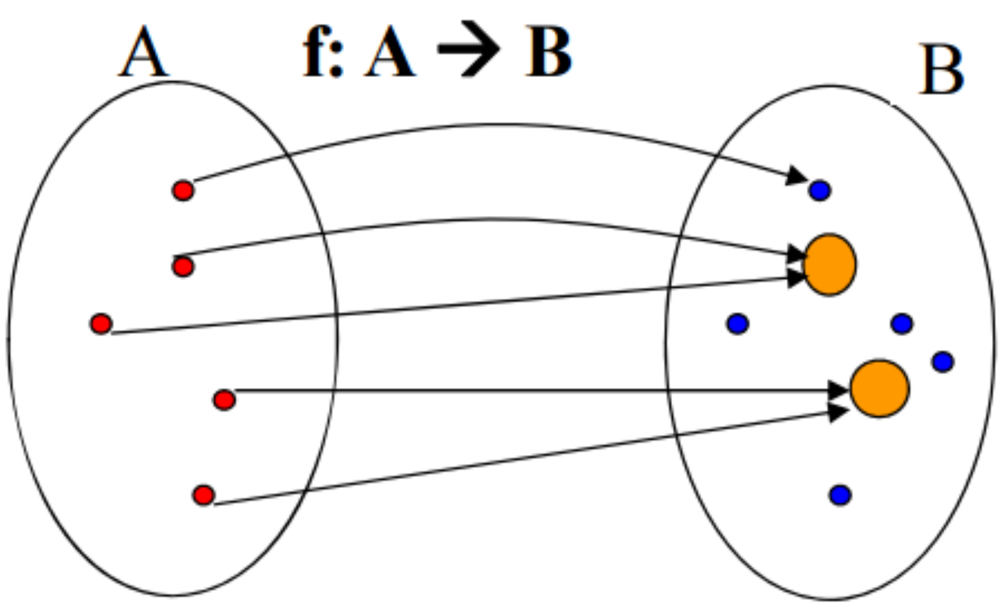


SUSTech

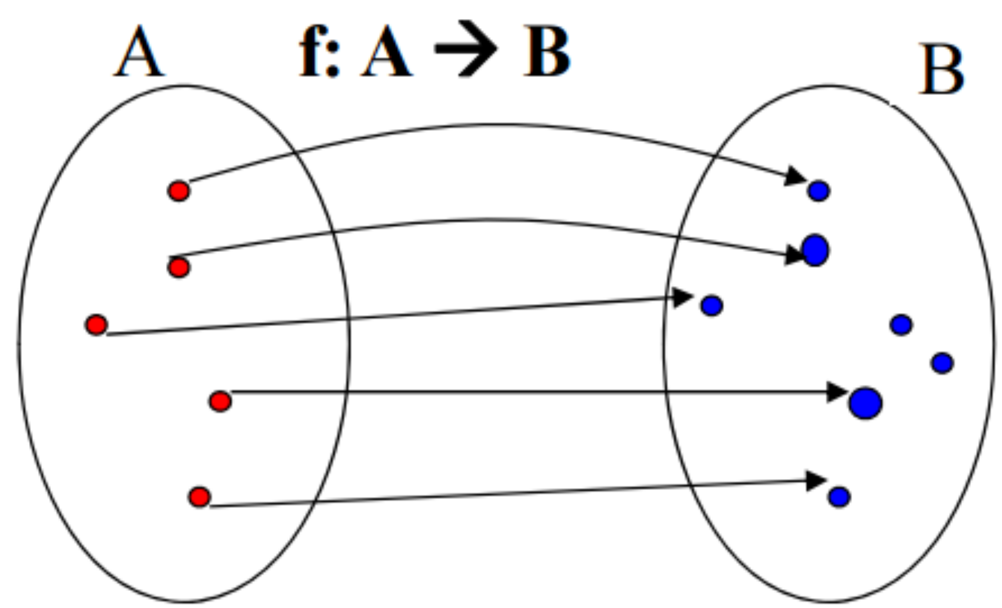
Injective (One-to-One) Functions

- A function f is called one-to-one or injective, if and only if $f(x) = f(y)$ implies $x = y$ for all x, y in the domain of f .
  In this case, f is called an injection.

- Alternatively: A function is one-to-one or injective if and only if $x \neq y$ implies $f(x) \neq f(y)$. * *contrapositive!*



Not injective



Injective function

Injective (One-to-One) Functions

- Examples:
  - Let $f : \{1, 2, 3\} \to \{a, b, c\}$, where $1 \mapsto c$, $2 \mapsto a$, $3 \mapsto c$. Is f injective?

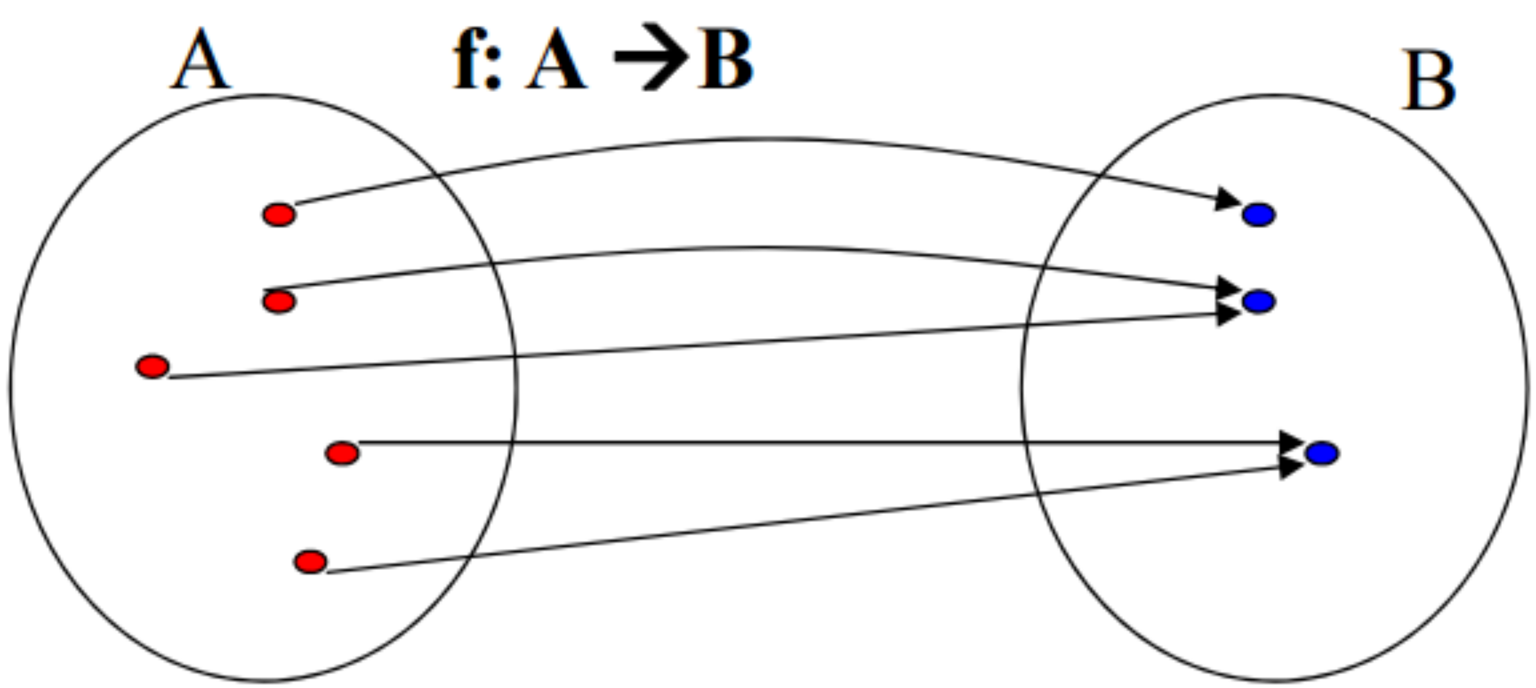
    No
  - Let $g : \mathbf{Z} \to \mathbf{Z}$, where $g(x) = 2x - 1$. Is g one-to-one?

    Yes
  - Let $h : \mathbf{Z} \to \mathbf{Z}$, where $h(x) = x^2 + 1$. Is h injective?

    No

Surjective (Onto) Functions

- A function f is called onto or surjective, if and only if for every $b \in B$ there is an element $a \in A$ such that $f(a) = b$. In this case, f is called a surjection.
- Alternatively: A function is onto or surjective if and only if all codomain elements are covered, i.e., $f(A) = B$.



Surjective (Onto) Functions

- Examples:
  - Let $f : \{1, 2, 3\} \to \{a, b, c\}$, where $1 \mapsto c$, $2 \mapsto a$, $3 \mapsto c$. Is f onto?

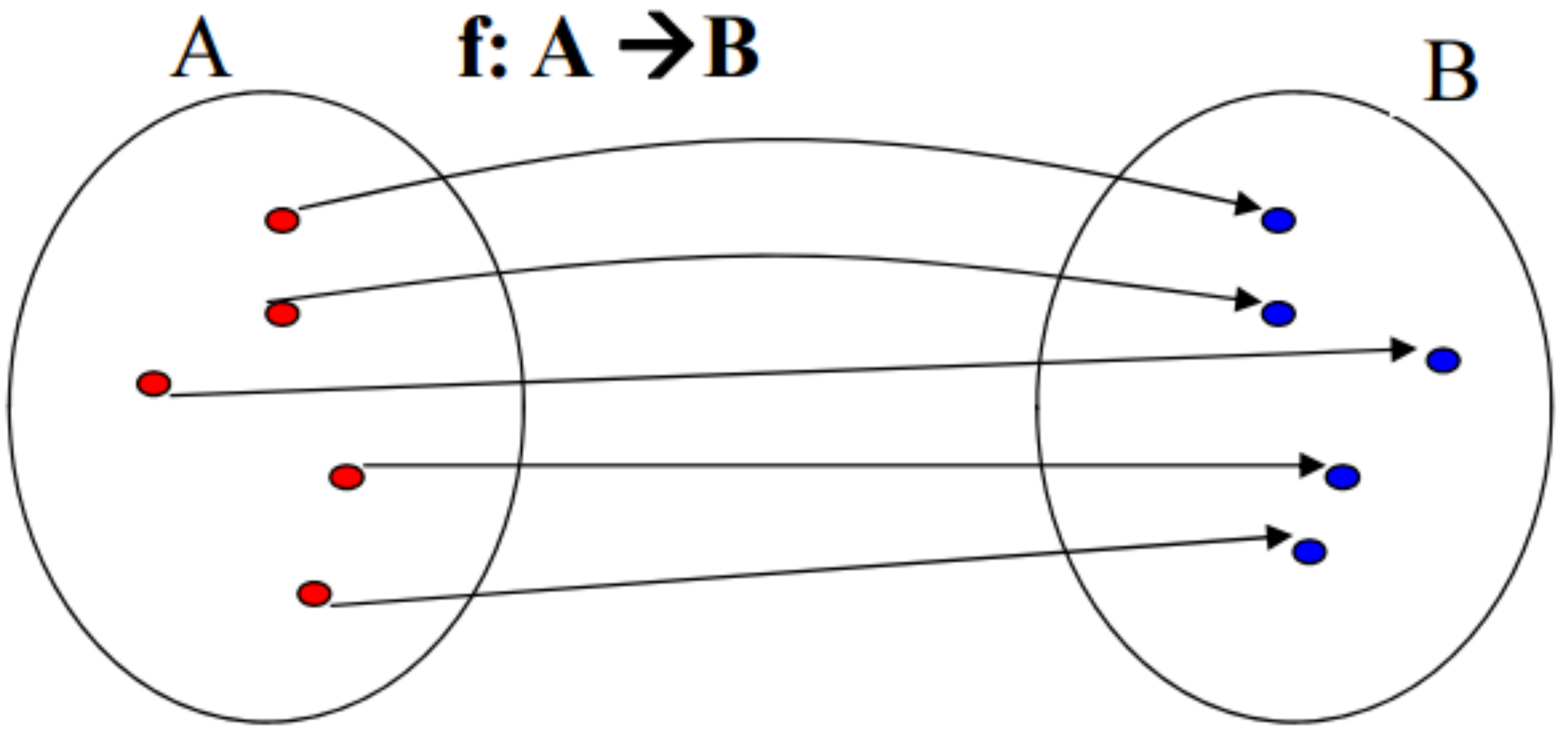
    No
  - Let $g : \mathbf{Z} \to \mathbf{Z}$, where $g(x) = 2x - 1$. Is g surjective?

    No
  - Let $h : \{1, 2, 3, 4\} \to \{0, 1, 2\}$, where $h(x) = x \bmod 3$. Is h onto?

    Yes

Bijective Functions

- A function f is called bijective, if and only if it is both one-to-one and onto, i.e., both injective and surjective.
  In this case, f is called a bijection.
  - Also known as a one-to-one correspondence.



Bijective Functions

- Examples:
  - Let $f : \{1, 2, 3\} \to \{a, b, c\}$, where $1 \mapsto c$, $2 \mapsto a$, $3 \mapsto b$. Is f bijective?

    Yes
  - Let $g : \mathbf{N} \to \mathbf{N}$, where $g(x) = \lfloor x/2 \rfloor$ (floor function). Is g bijective?

    No (not injective)
- The identity function on set A is the function $I_A : A \to A$ such that $I_A(a) = a$ for all $a \in A$, i.e., it assigns each element to itself. Identity functions are bijective functions.

Relevant Proof Strategy

- Consider a function $f : A \to B$.

To show that f is *injective* *(one-to-one)*	Show that for all $x, y \in A$ if $x \neq y$ then $f(x) \neq f(y)$
To show that f is not *injective*	Find specific $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$
To show that f is *surjective* *(onto)*	Show that for all $y \in B$ there exists $x \in A$ such that $f(x) = y$
To show that f is not *surjective*	Find a specific $y \in B$ such that $f(x) \neq y$ for all $x \in A$

SUSTech

Exercise *(3 mins)*

- **Theorem:** For an arbitrary function $f : A \to B$ with $|A| = |B| = n$, f is one-to-one if and only if f is onto. *Hint: prove "if" and "only if"*

To show that f is *injective (one-to-one)*	Show that for all $x, y \in A$ if $x \neq y$ then $f(x) \neq f(y)$
To show that f is not *injective*	Find specific $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$
To show that f is *surjective (onto)*	Show that for all $y \in B$ there exists $x \in A$ such that $f(x) = y$
To show that f is not *surjective*	Find a specific $y \in B$ such that $f(x) \neq y$ for all $x \in A$

SUSTech

Exercise *(3 mins)*

- **Theorem:** For an arbitrary function $f : A \rightarrow B$ with $|A| = |B| = n$, f is one-to-one if and only if f is onto. *Hint: prove "if" and "only if"*

- Proof:
  - "only if" part:

    Suppose that f is one-to-one. Let's do direct proof.
    Let $\{ x_1, x_2, \ldots , x_n \}$ be the n elements of A. Then since f is one-to-one, $f(x_i) \neq f(x_j)$ for $i \neq j$. Therefore, $|f(A)| = | \{ f(x_1), \ldots, f(x_n) \} | = n$.
    Since $|B| = n$ and $f(A) \subseteq B,$ we have $f(A) = B$.

  - "if" part:

    Suppose that f is onto. Let's use proof by contradiction.
    Let $A = \{x_1, x_2, \ldots , x_n \}$. If f is not injective, then there exist $x_i \neq x_j$ such that $f(x_i) = f(x_j)$. Then, $|f(A)| = | \{ f(x_1), \ldots, f(x_n) \} | \leq n - 1.$
    However, this contradicts with "f is onto" (i.e., $f(A) = B$, which implies $|f(A)| = |B| = n$). Therefore, f is one-to-one.

Note

- **Claim:** For an arbitrary function $f : A \rightarrow A$, f is one-to-one if and only if f is onto. ** what about this claim? still true?*

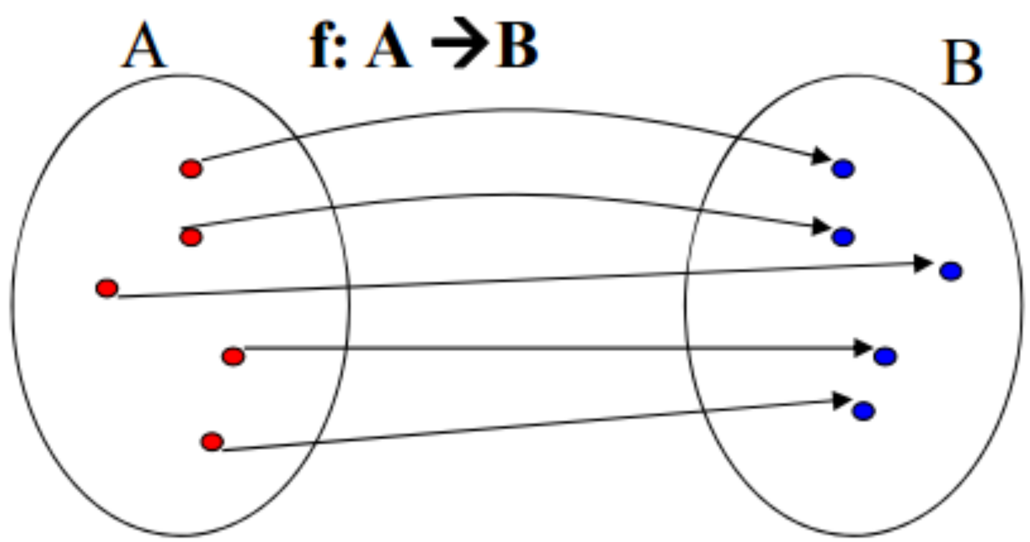
- **No!** Set A must be finite for the above **Claim** to be true.
  - Counterexample: $f : \boldsymbol{N} \rightarrow \boldsymbol{N}$, $f(x) = 2x$. Here f is one-to-one but not onto, e.g., 1 has no preimage.

Operations of Real-Valued Functions

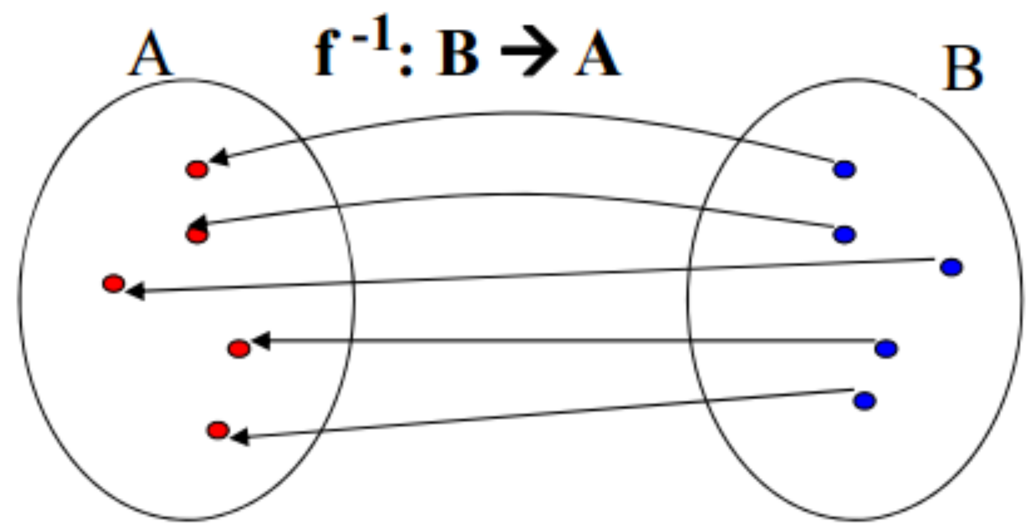
- Let f_1 and f_2 be functions from A to $\boldsymbol{R}$. Their sum $f_1 + f_2$ and product $f_1 f_2$ are also functions from A to $\boldsymbol{R}$ defined for all $x \in A$:
  - $(f_1 + f_2)(x) = f_1(x) + f_2(x)$
  - $(f_1 f_2)(x) = f_1(x) f_2(x)$
- Example: $f_1 = x - 1$, $f_2 = x^3 + 1$
  - $(f_1 + f_2)(x) = (x - 1) + (x^3 + 1) = x^3 + x$
  - $(f_1 f_2)(x) = (x - 1)(x^3 + 1) = x^4 - x^3 + x - 1$

Inverse Functions

- Let $f : A \rightarrow B$ be a bijection. The inverse of f is the function that assigns to $b \in B$ the unique element $a \in A$ such that $f(a) = b$, denoted by f^{-1}. Hence, $f^{-1}(b) = a$ when $f(a) = b$.
  In this case, f is called invertible.



f is bijective



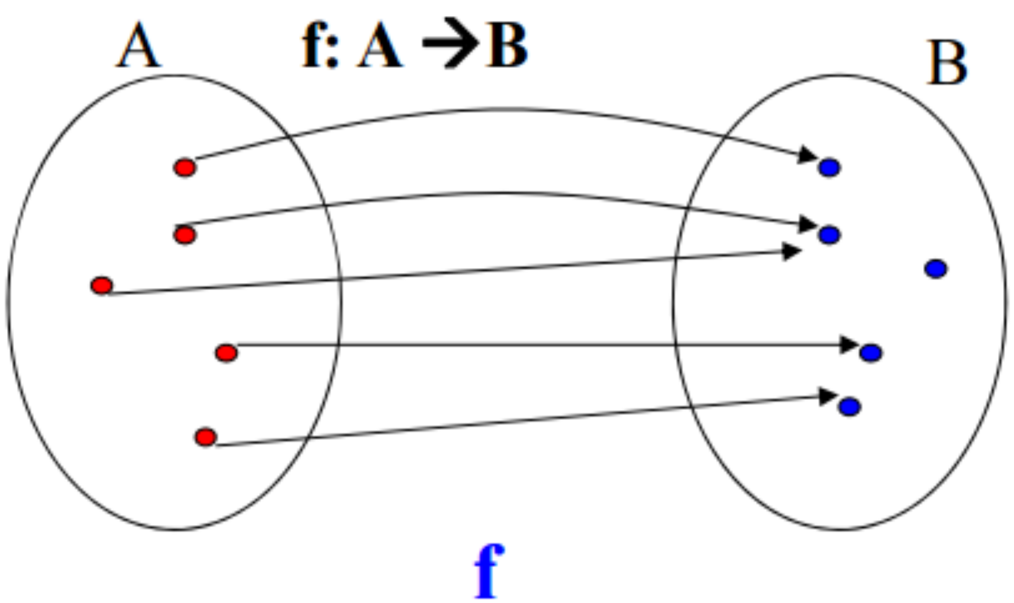
Inverse of f

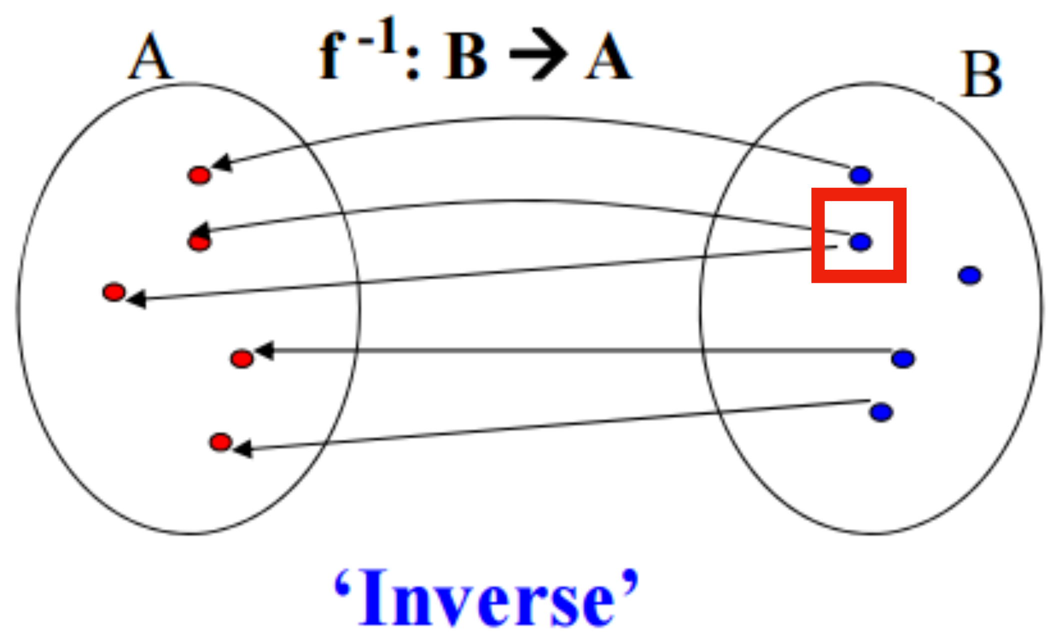
Inverse Functions

- **Theorem:** If *f* is not a bijection, then it is impossible to define the inverse function of *f*.

- Proof by cases:
  - **Case 1:** *f* is not injective

    The inverse is not a function: at least one element of *B* is mapped to two different elements of *A*



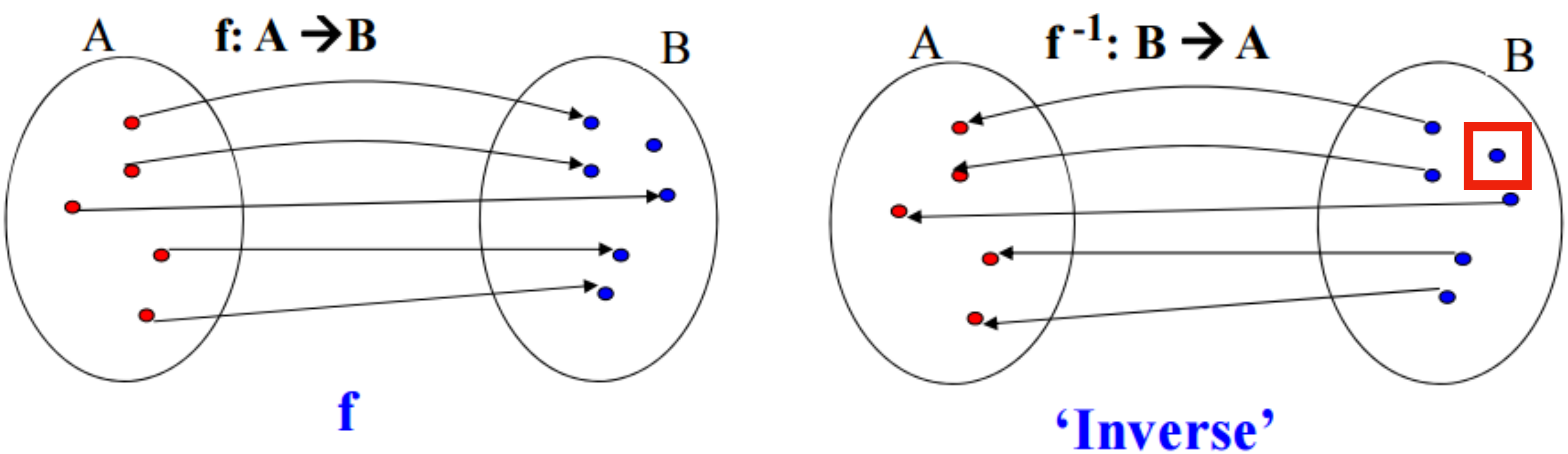


Inverse Functions

- **Theorem:** If *f* is not a bijection, then it is impossible to define the inverse function of *f*.

- Proof by cases:
  - **Case 2:** *f* is not surjective

    The inverse is not a function: at least one element of *B* is not mapped to any element of A



SUSTech

Inverse Functions

- Example 1:
  - $f : \boldsymbol{R} \rightarrow \boldsymbol{R}$, where $f(x) = 2x - 1$
  - What is the inverse function f^{-1}?

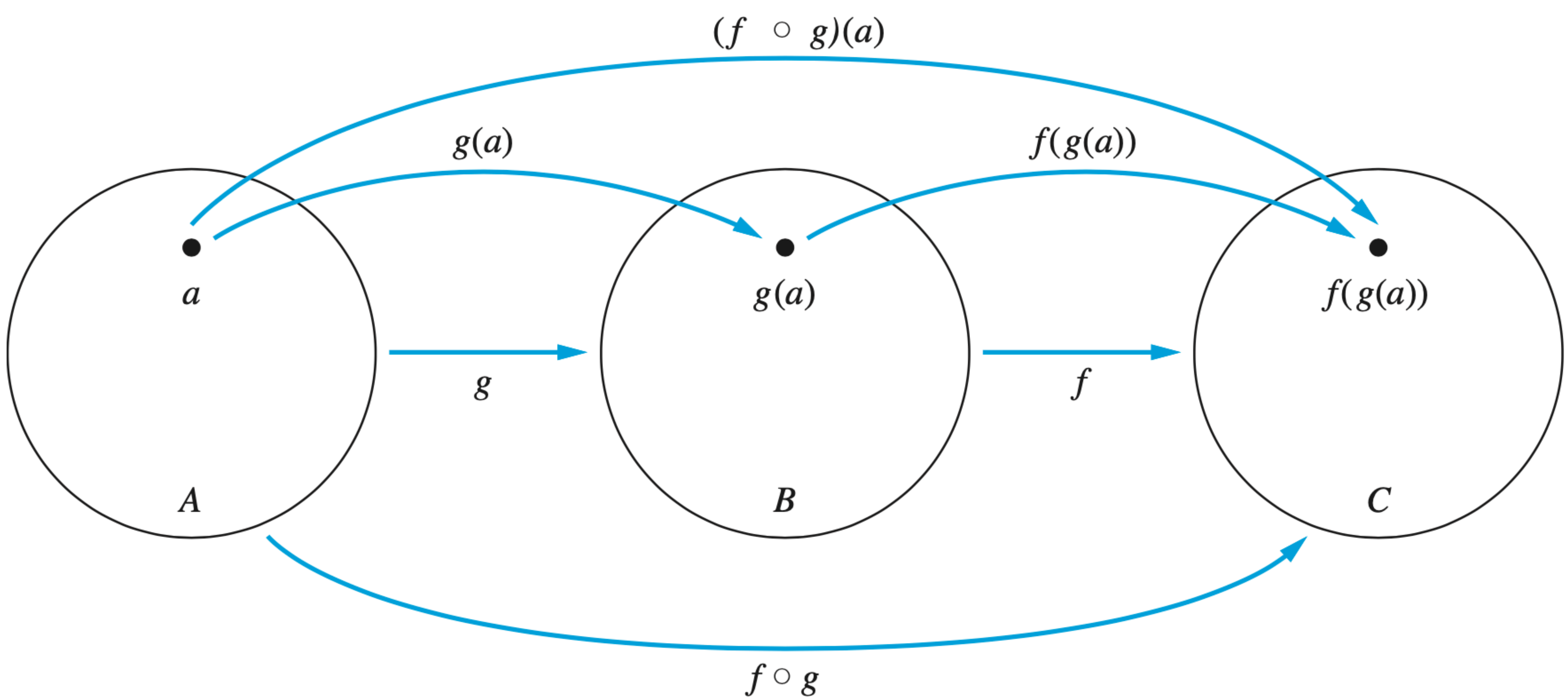
    $f^{-1}(x) = (x + 1)/2$

- Example 2:
  - $f : \boldsymbol{Z} \rightarrow \boldsymbol{Z}$, where $f(x) = 2x - 1$
  - Is f invertible?

    No, because f is not onto, e.g., 2 has no preimage.

Composition of Functions

- Consider two functions $f : B \to C$ and $g: A \to B$.
  The composition of the functions f and g, denoted by $f \circ g$, is defined as $(f \circ g)(x) = f(g(x))$.



Composition of Functions

- Example 1: $A = \{1, 2, 3\}$ and $B = \{a, b, c, d\}$
  - $f : A \to B$ where $1 \mapsto b, 2 \mapsto a, 3 \mapsto d$
  - $g : A \to A$ where $1 \mapsto 3, 2 \mapsto 1, 3 \mapsto 2$
  - What is $f \circ g$?

    $f \circ g : A \to B$ where $1 \mapsto d, 2 \mapsto b, 3 \mapsto a$

- Example 2:
  - $f : \mathbf{Z} \to \mathbf{Z}$ where $f(x) = 2x$
  - $g : \mathbf{Z} \to \mathbf{Z}$ where $g(x) = x^2$
  - What are $f \circ g$ and $g \circ f$?

    $(f \circ g)(x) = 2x^2$ $(g \circ f)(x) = 4x^2$ * *order of composition matters*

SUSTech

Composition of Functions

- **Theorem:** Suppose f is a bijection from A to B and let I_A and I_B respectively denote the identity functions on the sets A and B. Then,
  - $f^{-1} \circ f = I_A$
  - $f \circ f^{-1} = I_B$
- Proof: Consider any a, b such that $f(a) = b$
  - $(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a$
  - $(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b$

Some Important Functions

- The floor function assigns a real number x the largest integer that is $\leq x$, denoted by $\lfloor x \rfloor$.
- The ceiling function assigns a real number x the smallest integer that is $\geq x$, denoted by $\lceil x \rceil$.
- The factorial function f assigns a non-negative integer the product of the first n positive integers, denoted by $f(n) = n!$.
  - $0! = 1!/1 = 1$

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)	$\lceil x+n \rceil = \lceil x \rceil + n$

Exercise (3 mins)

- **Theorem:** If x is a real number, then $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + 1/2 \rfloor$.
  Hint: notice that $x = \lfloor x \rfloor + y$ for $0 \leq y < 1$ and prove it by cases

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)	$\lceil x + n \rceil = \lceil x \rceil + n$

Exercise *(3 mins)*

- **Theorem:** If x is a real number, then $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + 1/2 \rfloor$.
  Hint: notice that $x = \lfloor x \rfloor + y$ for $0 \le y < 1$ and prove it by cases

- Proof by cases:
  - By definition of floor function, $x = \lfloor x \rfloor + y$ where $\boldsymbol{0 \le y < 1}$.
  - **Case 1: $\boldsymbol{0 \le y < 1/2}$**

    We have $0 \le 2y < 1$ and $0 \le y + 1/2 < 1$, so

    $\lfloor 2x \rfloor = \lfloor 2\lfloor x \rfloor + 2y \rfloor = 2\lfloor x \rfloor + \lfloor 2y \rfloor = 2\lfloor x \rfloor$

    $\lfloor x + 1/2 \rfloor = \lfloor \lfloor x \rfloor + y + 1/2 \rfloor = \lfloor x \rfloor + \lfloor y + 1/2 \rfloor = \lfloor x \rfloor$
  - **Case 2: $\boldsymbol{1/2 \le y < 1}$**

    We have $1 \le 2y < 2$ and $1 \le y + 1/2 < 2$, so

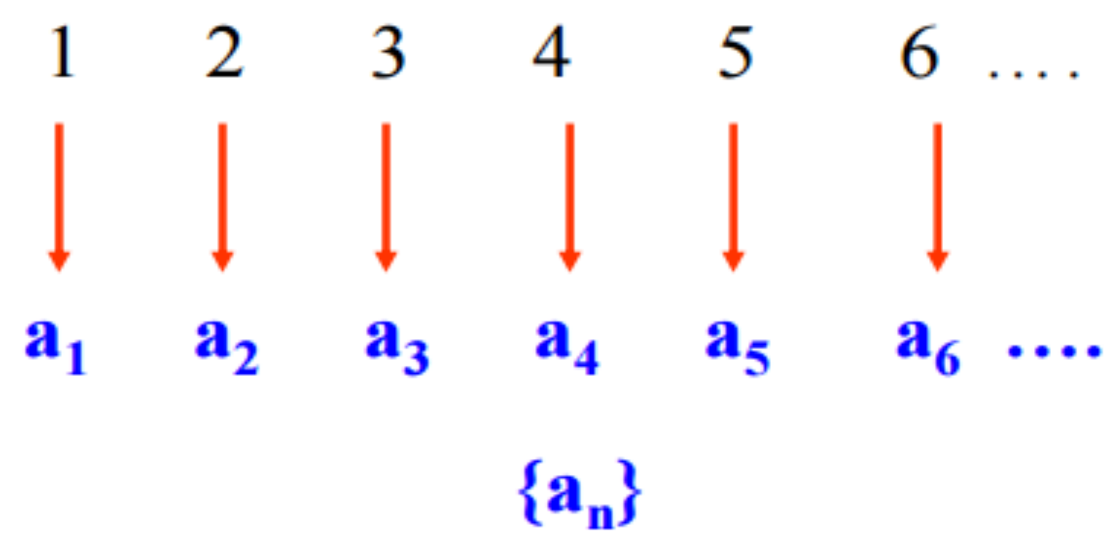
    $\lfloor 2x \rfloor = \lfloor 2\lfloor x \rfloor + 2y \rfloor = 2\lfloor x \rfloor + \lfloor 2y \rfloor = 2\lfloor x \rfloor + 1$

    $\lfloor x + 1/2 \rfloor = \lfloor \lfloor x \rfloor + y + 1/2 \rfloor = \lfloor x \rfloor + \lfloor y + 1/2 \rfloor = \lfloor x \rfloor + 1$

Sequences and Summations

Sequences

- A sequence is a function from a subset of the set of integers (usually $\{0, 1, 2, \ldots\}$ or $\{1, 2, 3, \ldots\}$) to a set S.



- Notations:
  - a_n denotes the image of the integer n
  - $\{a_n\}$ denotes the sequence $a_0, a_1, a_2, \ldots$ or $a_1, a_2, a_3, \ldots$
    ** note that here $\{a_n\}$ is not a set!*

SUSTech

Defining Sequences

- A sequence $\{a_n\}$ can be defined by providing explicit formulas for their terms, also called closed formulas.

- Examples:
  - $a_n = n^2$, where $n = 1, 2, 3, \ldots$
  - $a_n = (-1)^n$, where $n = 0, 1, 2, \ldots$

- Alternatively, the n-th element a_n can be defined recursively in terms of one or more previous elements. Such a recurrence relation together with initial conditions defines sequence $\{a_n\}$.

- Examples:
  - $a_n = a_{n-1} + 2$ for $n \geq 1$ and $a_0 = 1$
  - $f_n = f_{n-1} + f_{n-2}$ for $n \geq 2$ and $f_0 = 0, f_1 = 1$ ** Fibonacci sequence*

Arithmetic/Geometric Progression

- **Arithmetic progression:** a sequence of the form
$$a, a+d, a+2d, \ldots, a+nd, \ldots$$
where the initial term a and common difference d are real numbers.

- Example: $a_n = -1 + 4n$, where *n* = *0, 1, 2, 3, …*

- **Geometric progression:** a sequence of the form
$$a, ar, ar^2, \ldots, ar^n, \ldots$$
where the initial term a and common ratio r are real numbers.

- Example: $a_n = 3 \cdot (\frac{1}{2})^n$, where *n* = *0, 1, 2, 3, …*

Summations

- The summation of terms of a sequence is denoted by

$$\sum_{j=m}^{n} a_j = a_m + a_{m+1} + \cdots + a_n$$

- The variable j is referred to as the index of summation and the choice of the letter j is arbitrary.
  - m is the lower limit of the summation
  - n is the upper limit of the summation

- Useful summation identities:

$$\sum_{j=m}^{n} (ax_j + by_j) = a\sum_{j=m}^{n} x_j + b\sum_{j=m}^{n} y_j \qquad \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j = \sum_{i=1}^{m} a_i \sum_{j=1}^{n} b_j = \sum_{j=1}^{n} b_j \sum_{i=1}^{m} a_i$$

Summations

- The sum from the *0-th* term to the *n-th* term of the arithmetic progression $a, a+d, a+2d, \ldots, a+nd$ is

$$\sum_{j=0}^{n}(a+jd) = (n+1)a + d\sum_{j=0}^{n} j = (n+1)a + d\frac{n(n+1)}{2}$$

- The sum from the *0-th* term to the *n-th* term of of the geometric progression $a, ar, ar^2, \ldots, ar^n$ is

$$\sum_{j=0}^{n}(ar^j) = a\sum_{j=0}^{n} r^j = a\frac{r^{n+1}-1}{r-1}$$

What about the sum from the m-th term to the n-th term?

Summations

- The sum from the *m-th* term to the *n-th* term of the arithmetic progression $a + md, a + (m+1)d, \ldots, a + nd$ is

$$\sum_{j=m}^{n} (a + jd) = (n - m + 1)a + d\frac{(m+n)(n-m+1)}{2}$$

- The sum from the *m-th* term to the *n-th* term of the geometric progression $ar^m, ar^{m+1}, \ldots, ar^n$ is

$$\sum_{j=m}^{n} (ar^j) = a\sum_{j=m}^{n} r^j = a\frac{r^{n+1} - r^m}{r - 1}$$

Hint: can be proved directly or using $\sum_{j=m}^{n} = \sum_{j=0}^{n} - \sum_{j=0}^{m-1}$

Exercise *(2 mins)*

- Calculate the following summations:
  - $S = \sum_{j=1}^{5}(2+3j)$
  - $S = \sum_{j=3}^{5}(2+3j)$
  - $S = \sum_{i=1}^{4}\sum_{j=1}^{2}(2i-j)$
  - $S = \sum_{j=0}^{3} 2(5)^j$
  - $S = \sum_{i=1}^{4}\sum_{j=1}^{3} ij$

$$\sum_{j=m}^{n}(a+jd) = (n-m+1)a + d\frac{(m+n)(n-m+1)}{2} \qquad \sum_{j=m}^{n}(ar^j) = a\frac{r^{n+1}-r^m}{r-1}$$

SUSTech

Exercise *(2 mins)*

- Calculate the following summations:
  - $S = \sum_{j=1}^{5}(2+3j)$ 55
  - $S = \sum_{j=3}^{5}(2+3j)$ 42
  - $S = \sum_{i=1}^{4}\sum_{j=1}^{2}(2i-j)$ 28
  - $S = \sum_{j=0}^{3} 2(5)^j$ 312
  - $S = \sum_{i=1}^{4}\sum_{j=1}^{3} ij$ 60

$$\sum_{j=m}^{n}(a+jd) = (n-m+1)a + d\frac{(m+n)(n-m+1)}{2} \qquad \sum_{j=m}^{n}(ar^j) = a\frac{r^{n+1}-r^m}{r-1}$$

SUSTech

Infinite Series

- An infinite geometric series can be computed in the closed form for $|x| < 1$.

$$\sum_{k=0}^{\infty} x^k = \lim_{n\to\infty} \sum_{k=0}^{n} x^k = \lim_{n\to\infty} \frac{x^{n+1}-1}{x-1} = \frac{0-1}{x-1} = \frac{1}{1-x}$$

- Differentiating the above formula on both sides:

$$\sum_{k=0}^{\infty} kx^{k-1} = \frac{1}{(1-x)^2}$$

** proved true for $|x| < 1$ by a calculus theorem about infinite series*

  - Proof without calculus:

    Let $S_n = 1 + 2x + \ldots + nx^{n-1}$

    $(1-x)S_n = S_n - xS_n = 1 + x + \ldots + x^{n-1} - nx^n = (1-x^n)/(1-x) - nx^n$

    $S_n = (1-x^n)/(1-x)^2 - nx^n/(1-x) \to 1/(1-x)^2$ (if $n \to \infty$) * L'Hôpital's

Useful Summation Formulas

TABLE 2 Some Useful Summation Formulae.

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

Cardinality of Infinite Sets

Cardinality of Sets

- Recall that the cardinality of a finite set S is defined by the number of the elements in S, denoted by $|S|$.

- **Definition:** Sets A and B have the same cardinality if there is a one-to-one correspondence (bijection) between A and B, denoted by $|A| = |B|$.
  - Cardinality of infinite sets may be counter-intuitive, e.g., $|\boldsymbol{N}| = |\boldsymbol{Z}|$.

- **Definition:** If there exists a one-to-one (injective) function from A to B, then we say the cardinality of A is less than or equal to the cardinality of B, denoted by $|A| \leq |B|$. Moreover, if $|A| \leq |B|$ and A and B have different cardinalities, we say that the cardinality of A is less than the cardinality of B, denoted by $|A| < |B|$.

Schröder-Bernstein Theorem

- **Theorem:** If A and B are sets with $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$. That is, if there are injective functions $f : A \rightarrow B$ and $g : B \rightarrow A$, then there exists a bijective function between A and B. (Note that sets A and B can be infinite.)
  - *The proof is tricky and complicated so omitted here, but you can refer to the textbook [Exercise 41, page 187] if you are interested.*

- Example of its application: show that $|(0, 1)| = |(0, 1]|$
  - Proof:

    Construct two one-to-one functions:

    $f : (0, 1) \rightarrow (0, 1], f(x) = x$ * this means $|(0, 1)| \leq |(0, 1]|$

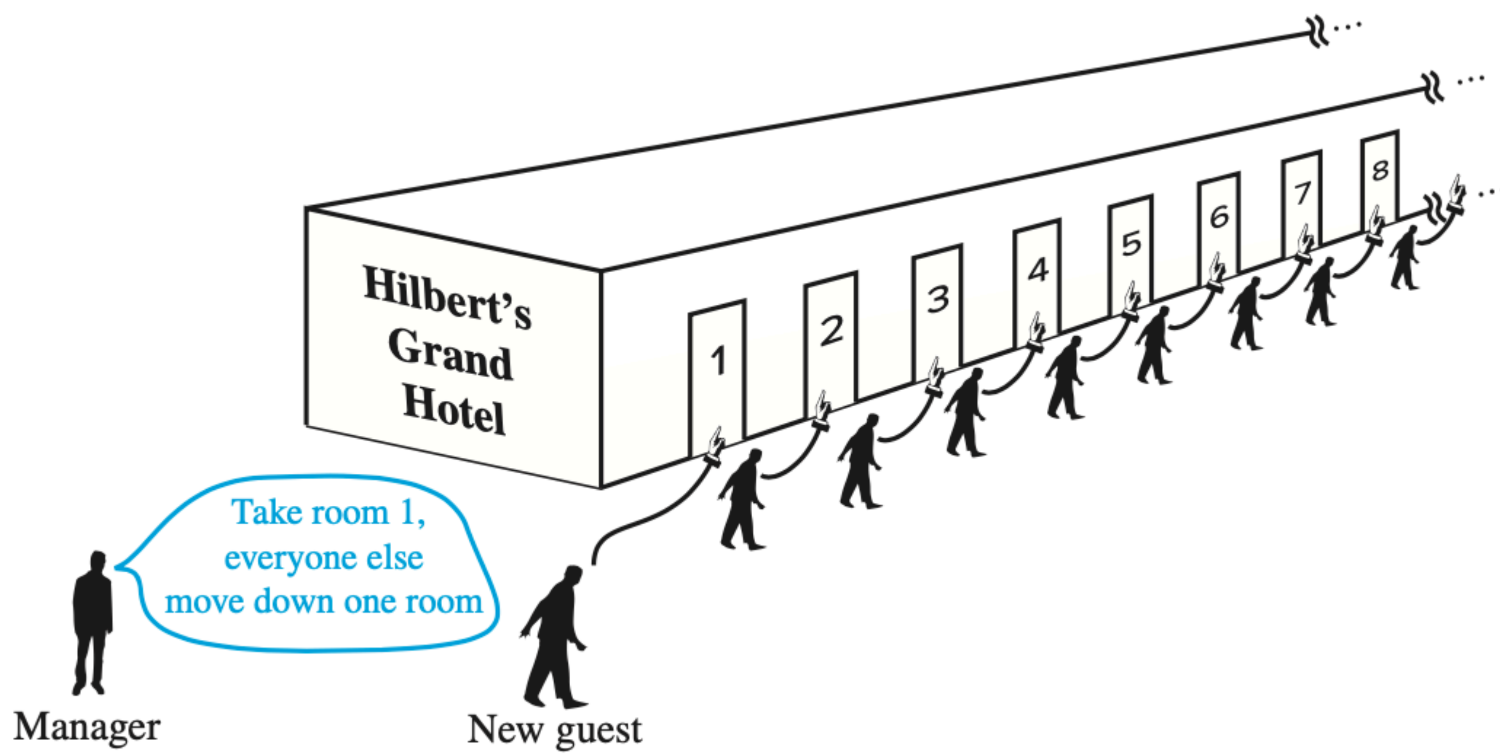
    $g : (0, 1] \rightarrow (0, 1), g(x) = x/2$ * this means $|(0, 1]| \leq |(0, 1)|$

Countable and Uncountable Sets

- **Definition:** A set that either is finite or has the same cardinality as $\boldsymbol{Z}^+$ is called countable, otherwise, it is called uncountable.
  - A countable set S can be infinite, but there must exist a bijection between $\boldsymbol{Z}^+$ and S.
- Intuitively, the cardinality of a countable set is less than that of any uncountable set. ** formal proof requires the axiom of choice*
- Why the name "countable"?
  - All elements in the countable set can be enumerated and listed just like listing positive numbers 1, 2, 3, …
  - There exists a list that can count any element in a countable set within finite steps.

Hilbert's Grand Hotel

- The Grand Hotel has countably infinite number of rooms, with each room occupied by a guest. We can always accommodate a new guest at this hotel.
    - This seems impossible because all rooms are already occupied. How can we accommodate the new guest?



    - Actually, you can even accommodate countably many new guests. How? ** this is left as an assignment problem*

SUSTech

Countable Sets: Example 1

- Example: $A = \{0, 2, 4, 6, \ldots\}$ ** is this set countable?*
  - (By definition) Is there a bijection between $\boldsymbol{Z}^+$ and A?
- Proof:
  - Define a function $f : \boldsymbol{Z}^+ \rightarrow A$, *where* $x \mapsto 2x - 2$.
  - Show f is a bijection!
  - **one-to-one:** if $f(x) = 2x - 2 = 2y - 2 = f(y)$, then $x = y$
  - **onto:** $\forall x \in A$, it has a preimage $(x + 2)/2$ in $\boldsymbol{Z}^+$
  - Therefore, A is countable.

Countable Sets: Example 2

- **Theorem:** "The set of integers $\boldsymbol{Z}$ is countable."
- Proof:
  - (Directly) List a sequence: $0, 1, -1, 2, -2, 3, -3, \ldots$
  - (Alternatively) Define a bijection from $\boldsymbol{Z}^+$ to $\boldsymbol{Z}$:

    when n is even: $f(n) = n/2$

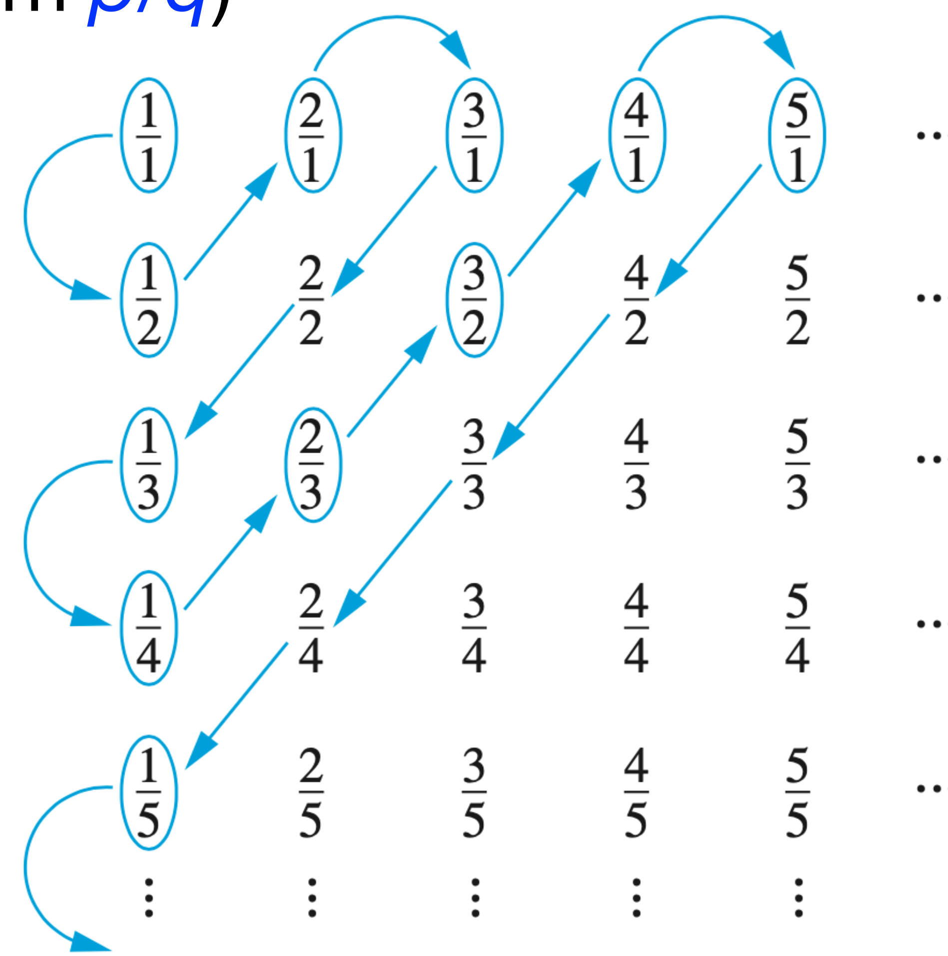
    when n is odd: $f(n) = -(n-1)/2$

SUSTech

Countable Sets: Example 3

- **Theorem:** "The set of rational numbers is countable."
- Proof: (rational numbers are of the form *p/q*)
  - List all positive rational numbers:
    1. list p/q with $p + q = 2$
       1/1
    2. list p/q with $p + q = 3$
       1/2, 2/1
    3. list p/q with $p + q = 4$
       3/1, ~~2/2,~~ 1/3

    …
  - Skip repeated (uncircled) numbers
  - Add 0 and negative numbers to the list
    0, 1, -1, 1/2, -1/2, 2, -2, 3, -3, 1/3, -1/3, …



Countable Sets: Example 4

- **Theorem:** "The set of finite strings S over a finite alphabet A is countable."
- Proof:
  - Define your favorite alphabetical order for symbols in A
  - We show that the finite strings in S can be listed in a sequence:
    1. list all the strings of length 0 in alphabetical order
    2. list all the strings of length 1 in alphabetical order
    3. list all the strings of length 2 in alphabetical order

    …
  - This implies a bijection from $\mathbf{Z}^+$ to S.

SUSTech

Exercise *(3 mins)*

- **Theorem:** "The set of all Java programs is countable."

  - **Theorem:** "The set of finite strings S over a finite alphabet A is countable."
  - Proof:
    - Define your favorite alphabetical order for symbols in A
    - We show that the finite strings in S can be listed in a sequence:
      1. list all the strings of length 0 in alphabetical order
      2. list all the strings of length 1 in alphabetical order
      3. list all the strings of length 2 in alphabetical order

      …
    - This implies a bijection from $\boldsymbol{Z}^+$ to S.

Exercise *(3 mins)*

- **Theorem:** "The set of all Java programs is countable."
- Proof:
  - Let S be the set of finite strings constructed from the finite alphabet that consists of all characters that may appear in a Java program. Define any alphabetical order for such characters. Then, as proved in the previous theorem, we can enumerate strings in S.
  - For each enumerated string s, do the following:
    - feed s into a Java compiler
    - if the complier says YES (i.e., s is a syntactically correct Java program), we add s to the list, otherwise, skip it
    - move on to the next string
  - This implies a bijection from $\boldsymbol{Z}^+$ to the set of all Java programs.

SUSTech

Uncountable Sets

- **Theorem:** "The set of real numbers $\boldsymbol{R}$ is uncountable."
- Proof by contradiction: (Cantor's diagonal argument)
  - Assume that $\boldsymbol{R}$ is countable.
    Then, every subset of $\boldsymbol{R}$ is countable (why?). In particular, interval $[0, 1]$ is countable. This implies that there exists a list $r_1, r_2, r_3, \ldots$ that can enumerate all elements in this set, where

    $r_1 = 0.\mathbf{d_{11}}d_{12}d_{13}d_{14}\cdots$

    $r_2 = 0.d_{21}\mathbf{d_{22}}d_{23}d_{24}\cdots$

    $r_3 = 0.d_{31}d_{32}\mathbf{d_{33}}d_{34}\cdots$

    $\ldots$

    with $d_{i\,j} \in \{0, 1, 2, \ldots, 9\}$ ** note that $1 = 0.999999\cdots$*
  - Construct a real number r that is not included in the above list:

    $r = 0.d_1d_2d_3d_4\cdots$ *where* $d_i \neq \mathbf{d_{ii}}$

SUSTech

Exercise (3 mins)

- **Theorem:** "The power set $\mathcal{P}(\boldsymbol{N})$ is uncountable."
  *Recall that $\mathcal{P}(\boldsymbol{N})$ contains all subsets of **N***

- **Theorem:** "The set of real numbers $\boldsymbol{R}$ is uncountable."
- Proof by contradiction: (Cantor's diagonal argument)
  - Assume that $\boldsymbol{R}$ is countable.
    Then every subset of $\boldsymbol{R}$ is countable, in particular, the interval $[0, 1]$ is countable. This implies that there exists a list $r_1, r_2, r_3, \ldots$ that can enumerate all elements of this set, where

    $r_1 = 0.\mathbf{d_{11}}d_{12}d_{13}d_{14} \cdots$

    $r_2 = 0.d_{21}\mathbf{d_{22}}d_{23}d_{24} \cdots$

    $r_3 = 0.d_{31}d_{32}\mathbf{d_{33}}d_{34} \cdots$

    $\ldots$

    with $d_{ij} \in \{0, 1, 2, \ldots, 9\}$ *Note that $1 = 0.999999\cdots$*
  - Construct a real number r that is not included in the above list:

    $r = 0.d_1d_2d_3d_4 \cdots$ *where* $d_i \neq \mathbf{d_{ii}}$

Exercise (3 mins)

- **Theorem:** “The power set $\mathcal{P}(\boldsymbol{N})$ is uncountable.”

- Proof by contradiction: (Cantor’s diagonal argument)
  - Assume that $\mathcal{P}(\boldsymbol{N})$ is countable.
    This means that all elements of this set can be listed as $S_0, S_1, S_2, \ldots$, where $S_i \in \mathcal{P}(\boldsymbol{N})$. Then, each $S_i \subseteq \boldsymbol{N}$ can be represented by a bit string $b_{i0}b_{i1}b_{i2}\cdots$, where $b_{i\,j} = 1$ if $j \in S_i$ and $b_{i\,j} = 0$ if $j \notin S_i$:

    $S_0 = \boldsymbol{b_{00}}b_{01}b_{02}b_{03}\cdots$

    $S_1 = b_{10}\boldsymbol{b_{11}}b_{12}b_{13}\cdots$

    $S_2 = b_{20}b_{21}\boldsymbol{b_{22}}b_{23}\cdots$

    $\ldots$

    with $b_{ij} \in \{0, 1\}$ for $i, j \in \boldsymbol{N}$

  - Construct a set $S \in \mathcal{P}(\boldsymbol{N})$ that is not included in the above list:

    $S = b_0b_1b_2b_3\cdots$ where $b_i \neq \boldsymbol{b_{ii}}$

SUSTech

Computable vs Uncomputable

- **Definition:** We say that a function is computable if there is a computer program in some programming language that finds the values of this function. If a function is not computable, we say it is uncomputable.

- **Theorem:** "There exist uncomputable functions." ** very cool!*

- Proof sketch:
  - **Part 1:** The set of all computer programs in all programming languages is countable. ** why?*
  - **Part 2:** The set of all functions from $\mathbf{Z}^+$ to $\{0, 1, \ldots, 9\}$ is uncountable. ** why?*
  - **Conclusion:** there exists a function $f^* : \mathbf{Z}^+ \rightarrow \{0, 1, \ldots, 9\}$ that cannot be computed by any computer program, i.e., f^* is uncomputable. ** proof by contradiction*

SUSTech

The Continuum Hypothesis

- We know that $|\boldsymbol{N}| < |\mathcal{P}(\boldsymbol{N})|$, because $|\boldsymbol{N}| \leq |\mathcal{P}(\boldsymbol{N})|$, $\boldsymbol{N}$ is countable while $\mathcal{P}(\boldsymbol{N})$ is uncountable.
  - **Cantor's theorem:** $|S| < |\mathcal{P}(S)|$ holds for any set S
- **Q:** Is there a set A such that $|\boldsymbol{N}| < |A| < |\mathcal{P}(\boldsymbol{N})|$?
- **Continuum hypothesis:** The above set A does not exist!
  - This is a very important open problem in mathematics.

04 Complexity of Algorithms

To be continued…

Assignment 2 and Quizzes

- Deadline for Assignment 2: Oct 25
- Quiz 1 will take place in class on Oct 12 and it captures materials from 02 Logic and Proofs to 03 Sets and Functions.
- We will have 2 open-book quizzes in total for this course:
  - 3~6 questions in ~20 minutes for each quiz.
  - Must attend the quizzes in person.
  - Please bring several pieces of paper to write your answers on.
  - No electronic device is allowed during the quiz.
  - After quiz, please take photos of your quiz answers and submit to Blackboard (you will have ~5 minutes after quiz to do this).

SUSTech