# 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

○ Answer: axiomatic set theory (e.g., Zermelo–Fraenkel set theory)

  * out of scope of this course
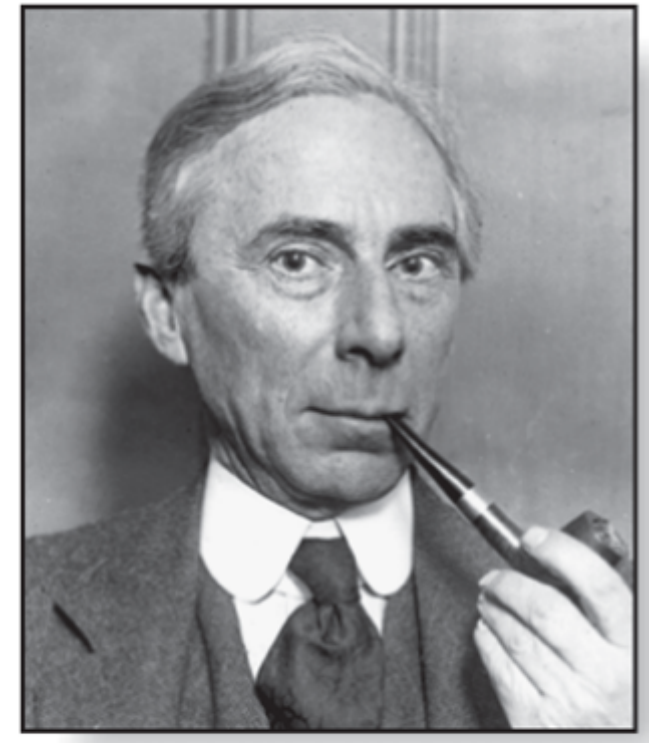
Bertrand Russell (1872-1970)
Cambridge, UK
Nobel Prize Winner

SUSTech

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

- ...

SUSTech

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

SUSTech

Important Sets

- Natural numbers: $N = \{0, 1, 2, 3, ...\}$

- Integers: $Z = \{..., -2, -1, 0, 1, 2, ...\}$

- Positive integers: $Z^+ = \{1, 2, 3, ...\}$

- Rational numbers: $Q = \{p/q \mid p, q \in Z, q \neq 0\}$

- Real numbers: R

- Complex numbers: $C = \{a + bi \mid a, b \in R\}$

Interval Notation

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

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

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

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

SUSTech

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 $\varnothing \neq \{\varnothing\}$

○ A set can be visualized using Venn diagrams
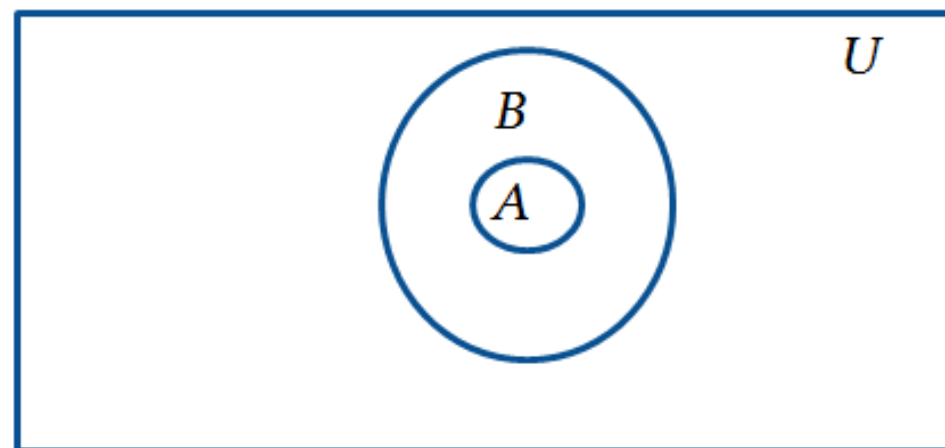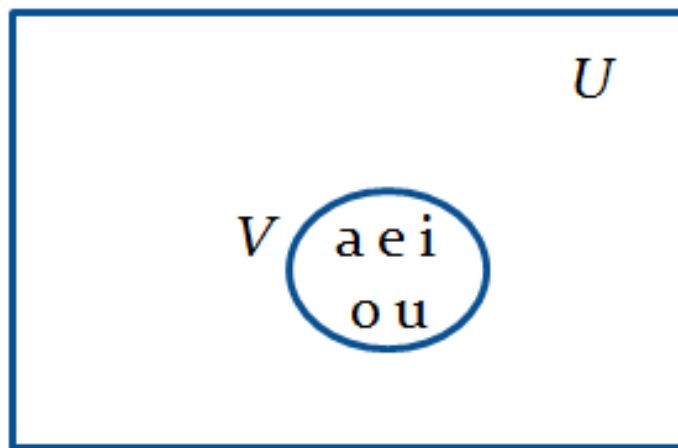
John Venn (1834-1923)
Cambridge, UK

SUSTech

Subsets and Proper Subsets

○ A set *A* is called a subset of *B,* denoted by *A* ⊆ *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* ⊆ *B* but *A* ≠ *B*, then we say *A* is a proper subset of *B*, denoted by *A* ⊂ *B*, i.e., $\forall x \, (x \in A \rightarrow x \in B) \land \exists x \, (x \in B \land x \notin A)$

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

$$A = B \quad \textit{iff} \quad A \subseteq B \textit{ and } B \subseteq A$$

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

SUSTech

Subset Properties

○ **Theorem:** $\varnothing \subseteq S$

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

○ **Theorem:** $S \subseteq S$

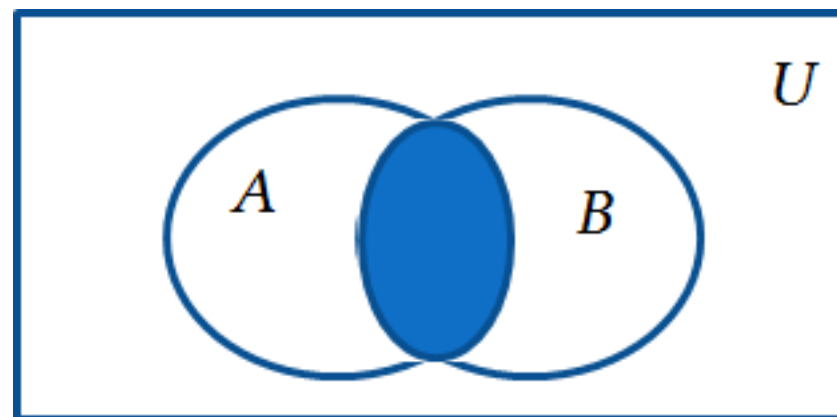○ Proof: By definition, we need to prove $\forall x(x \in S \rightarrow x \in S)$, which is obviously true.

SUSTech

Set Operations

○ **Union:** The union of sets *A* and *B*, denoted by *A* ∪ *B*, is the set *{x | x ∈ A ∨ x ∈ B}*.
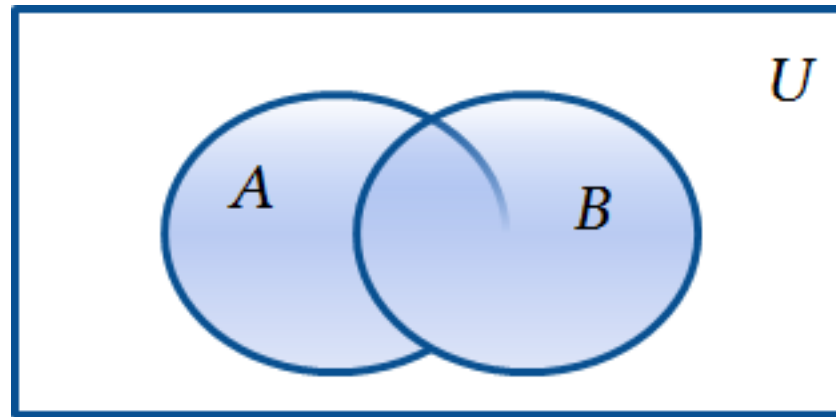
Venn Diagram for $A \cup B$

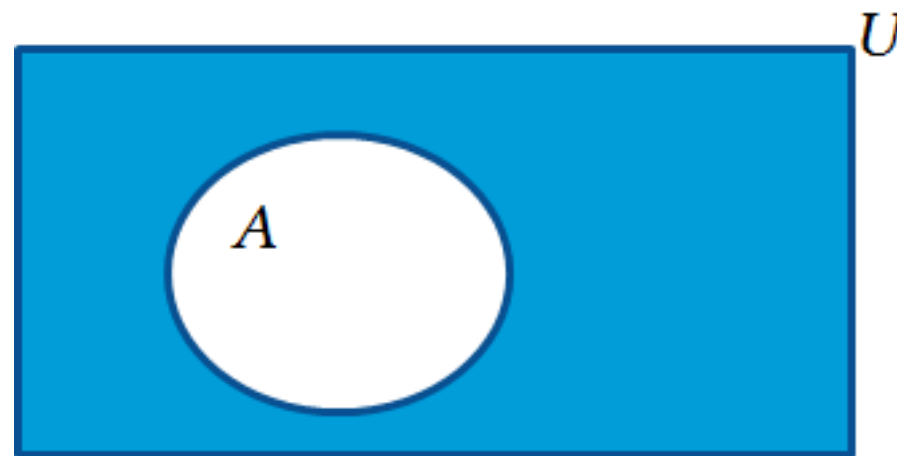○ **Intersection:** The intersection of sets *A* and *B*, denoted by *A* ∩ *B*, is the set *{x | x ∈ A ∧ x ∈ B}*. Two sets *A* and *B* are called disjoint if their intersection is empty, i.e., *A* ∩ *B* = ∅.

Venn Diagram for $A \cap B$

SUSTech

Set Operations

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

Venn Diagram for $A \cup B$

○ **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., $A - B = \{x \mid x \in A \land x \notin B\} = A \cap \bar{B}$

Venn Diagram for $A \cap B$

SUSTech
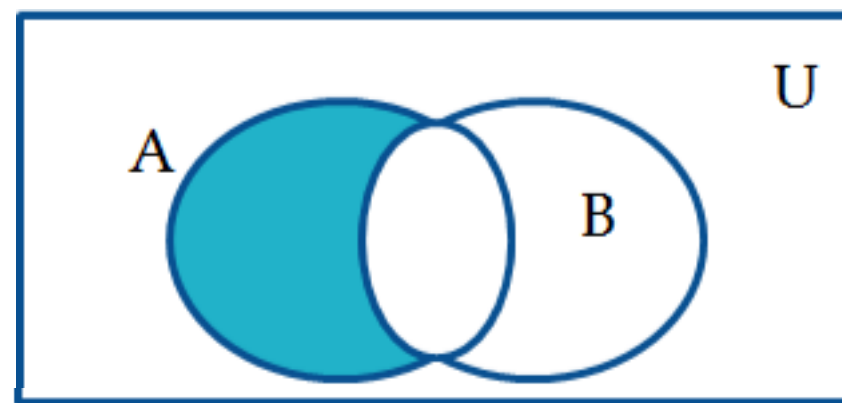
Exercise *(1 min)*

U = {0, 1, …, 10}, A = {1, 2, 3, 4, 5}, B = {4, 5, 6, 7, 8}

○ $A \cup B$

○ $A \cap B$

○ $\bar{A}$

○ $\bar{B}$

○ $A - B$

○ $B - A$

SUSTech

Unions and Intersections (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: $\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$.

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

SUSTech

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

- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

SUSTech

Set Identities

○ Absorption laws

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

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

○ Complement laws

- $A \cup \bar{A} = U$

- $A \cap \bar{A} = \varnothing$

○ 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…

SUSTech

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

○ Using membership tables: ** requires tedious calculations*

A	B	$\bar{A}$	$\bar{B}$	$\overline{A \cap B}$	$\bar{A} \cup \bar{B}$
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 | x ∈ $\overline{A \cap B}$}   *definition*

= {x | x ∉ A ∩ B}   *definition of complement*

= {x | ¬(x ∈ (A ∩ B))}   *definition*

= {x | ¬(x ∈ A ∧ x ∈ B)}   *definition of intersection*

= {x | ¬(x ∈ A) ∨ ¬(x ∈ B)}   *De Morgan's*

= {x | x ∉ A ∨ x ∉ B}   *definition*

= {x | x ∈ $\bar{A}$ ∨ x ∈ $\bar{B}$)}   *definition of complement*

= {x | x ∈ $\bar{A}$ ∪ $\bar{B}$}   *definition of union*

= $\bar{A} \cup \bar{B}$ *definition*

○ Using logical equivalence without set builders: ** less elegant*

• Show $\forall x(x \in \overline{A \cap B} \leftrightarrow x \in \bar{A} \cup \bar{B})$ ** see the textbook for details*

18

SUSTech

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, …, 20}* ($|A| = 20$)

- *B = {1, 2, 3, …}* (infinite)

- $|\varnothing| = 0$

○ **Cardinality of the union:** $|A \cup B| = |A| + |B| - |A \cap B|$ ** why?*

- $|A \cap B|$ counted twice in $|A| + |B|$

- known as the inclusion-exclusion principle for 2 sets

SUSTech

Tuples

○ An *n*-tuple *(a₁, a₂, …, aₙ)* 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
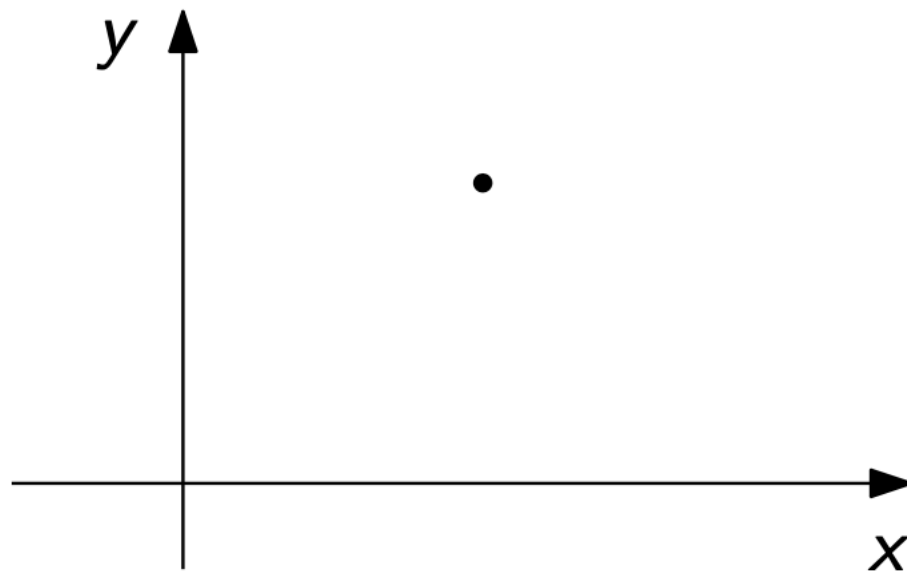
Cartesian Product

○ 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: $A = \{1, 2\}$, $B = \{a, b, c\}$

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

○ $A \times B \neq B \times A$ *order matters*

○ $|A \times B| = |A| \times |B|$ if A, B are finite sets

SUSTech

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 follows:

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

○ Example: $A = \{0, 1\}$, $B = \{1, 2\}$, $C = \{0, 1, 2\}$

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

SUSTech

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:

  - $\varnothing$ *$\mathcal{P}(\varnothing) = \varnothing$*

  - *{1}*   *$\mathcal{P}(\{1\}) = \{\varnothing, \{1\}\}$*

  - *{1, 2}*   *$\mathcal{P}(\{1,2\}) = \{\varnothing, \{1\}, \{2\}, \{1,2\}\}$*

  - *{1, 2, 3}*   *$\mathcal{P}(\{1,2,3\}) = \{\varnothing, \{1\}, \{2\}, \{3\} \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$*

- 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: $A \vee B = \{1, 2, 5\} = 11001$

- Intersection: $A \wedge B = \{5\} = 00001$

- Complement: $\bar{A} = \{1, 3, 4\} = 10110$

* set operations are converted to bitwise operations of Boolean algebra

SUSTech

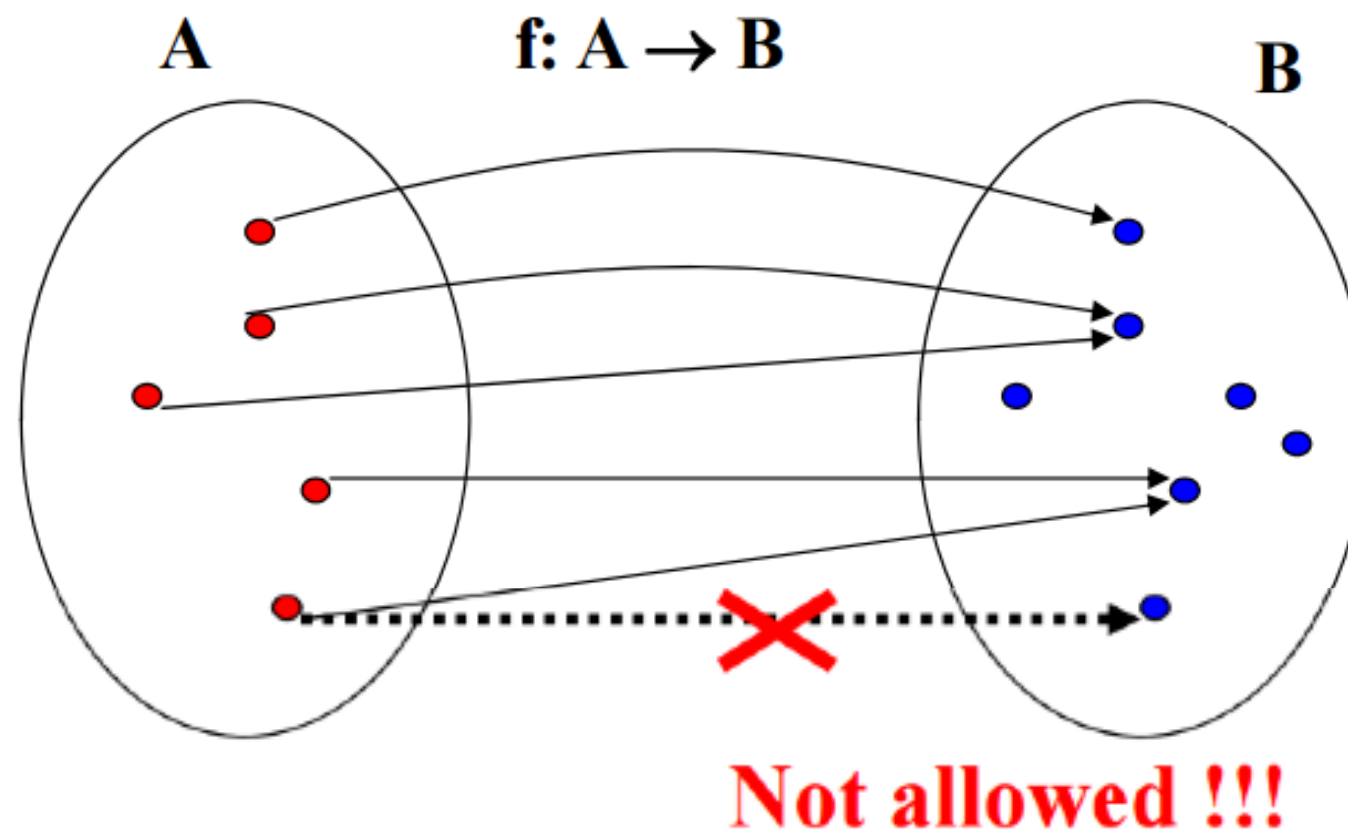# Functions

Functions

○ Let *A* and *B* be two sets. A function from *A* to *B*, denoted by *f : A → 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
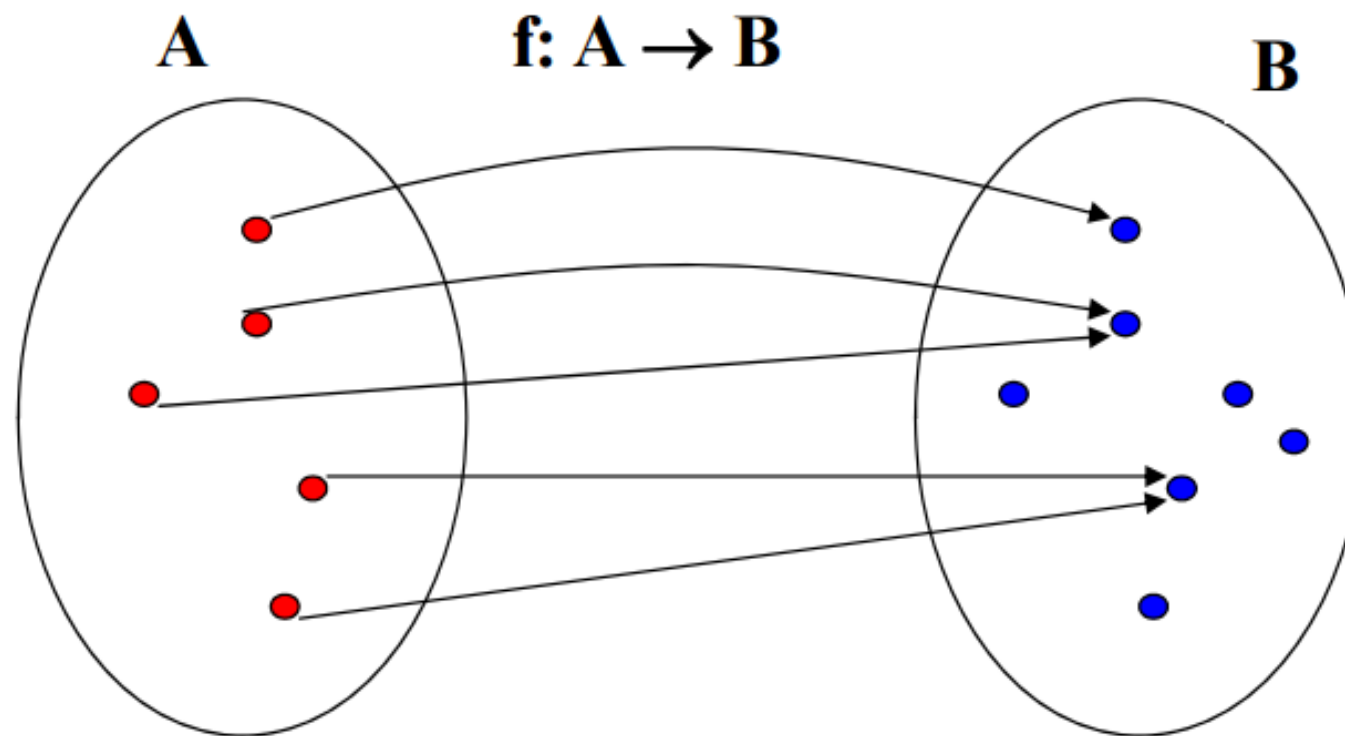
Functions

○ Let *A* and *B* be two sets. A function from *A* to *B*, denoted by
  f : A → 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

Representing Functions

○ Representing functions *f : A → 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 ↦ c, 2 ↦ a, 3 ↦ c*. Is *f* a function?
  Yes

  g is defined as *1 ↦ c, 1 ↦ b, 2 ↦ a, 3 ↦ c*. Is *g* a function?
  No

- *A = {0, 1, … , 9}, B = {0, 1, 2}*

  h is defined as *h(x) = x* mod *3*. Is *h* a function?
  Yes

SUSTech

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: *A = {1, 2, 3}, B = {a, b, c}*

- the image of *1* is *c*

- *2* is a preimage of *a*

- the domain of *f* is *{1, 2, 3}*

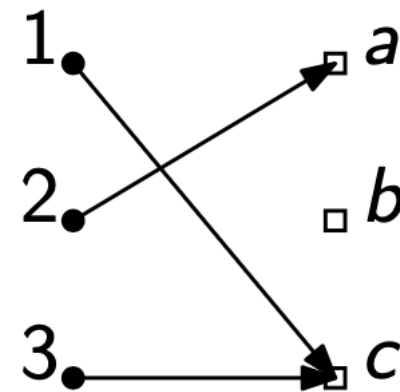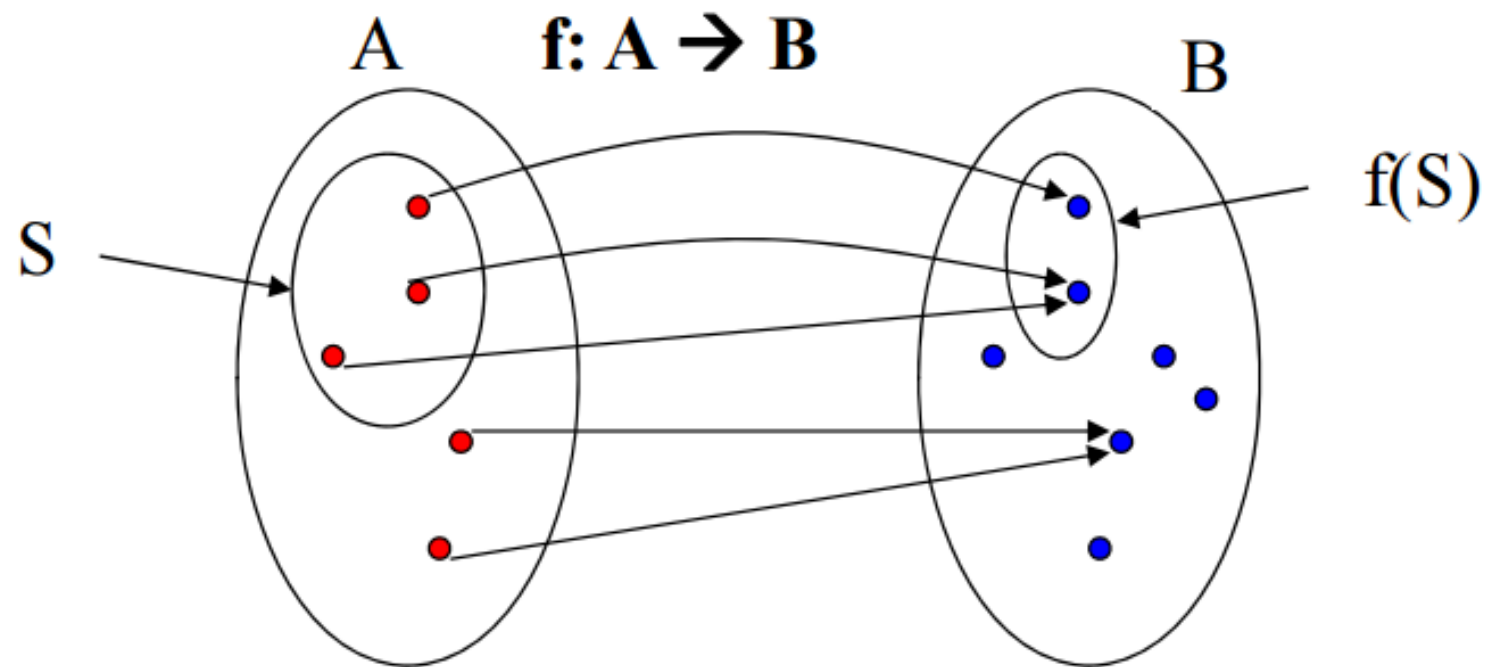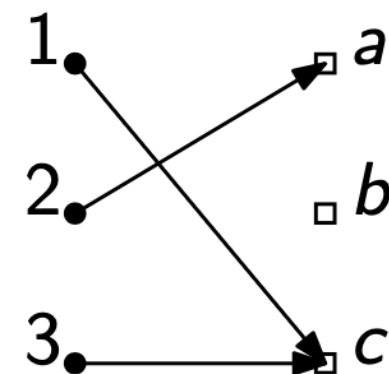- the codomain of *f* is *{a, b, c}*

- the range of *f* is *{a, c}*

Image of a Subset

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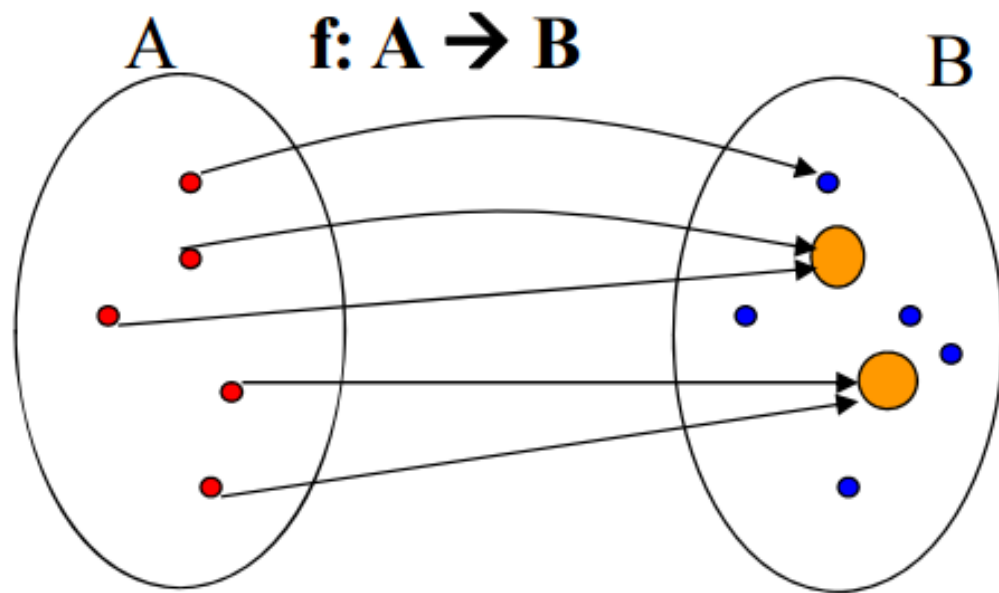

○ Example: Let $S = \{1, 3\}$, what is $f(S)$?

• $f(S) = \{c\}$

SUSTech

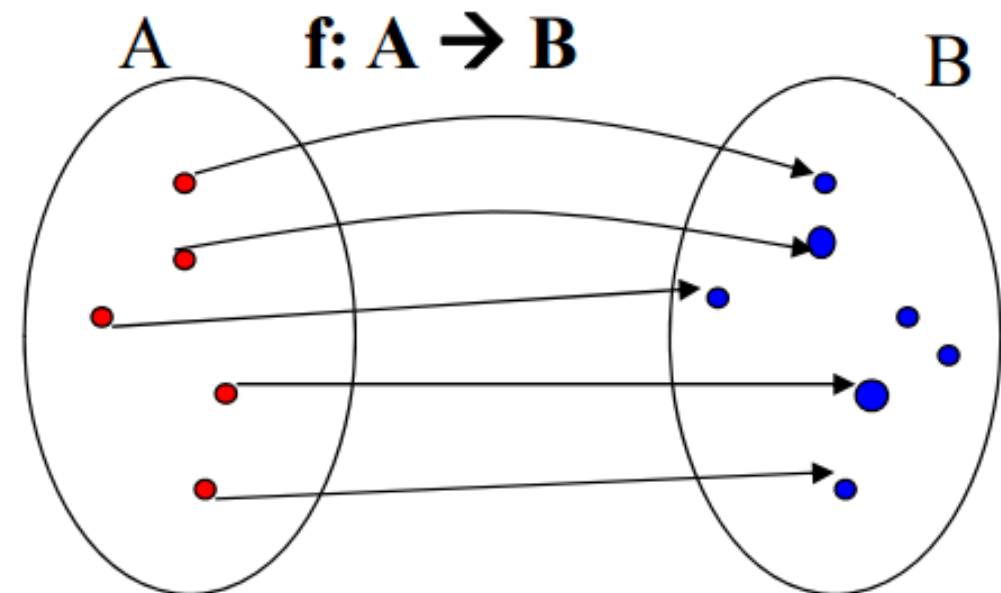# Injective (One-to-One) Functions

○ 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 ≠ y* implies *f(x) ≠ f(y)*. * *contrapositive!*

Not injective

Injective function

Injective 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

SUSTech

Surjective (Onto) Functions

○ A function *f* is called onto or surjective, if and only if for every *b* ∈ *B* there is an element *a* ∈ *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*.

A   f: A ➔ B   B

SUSTech
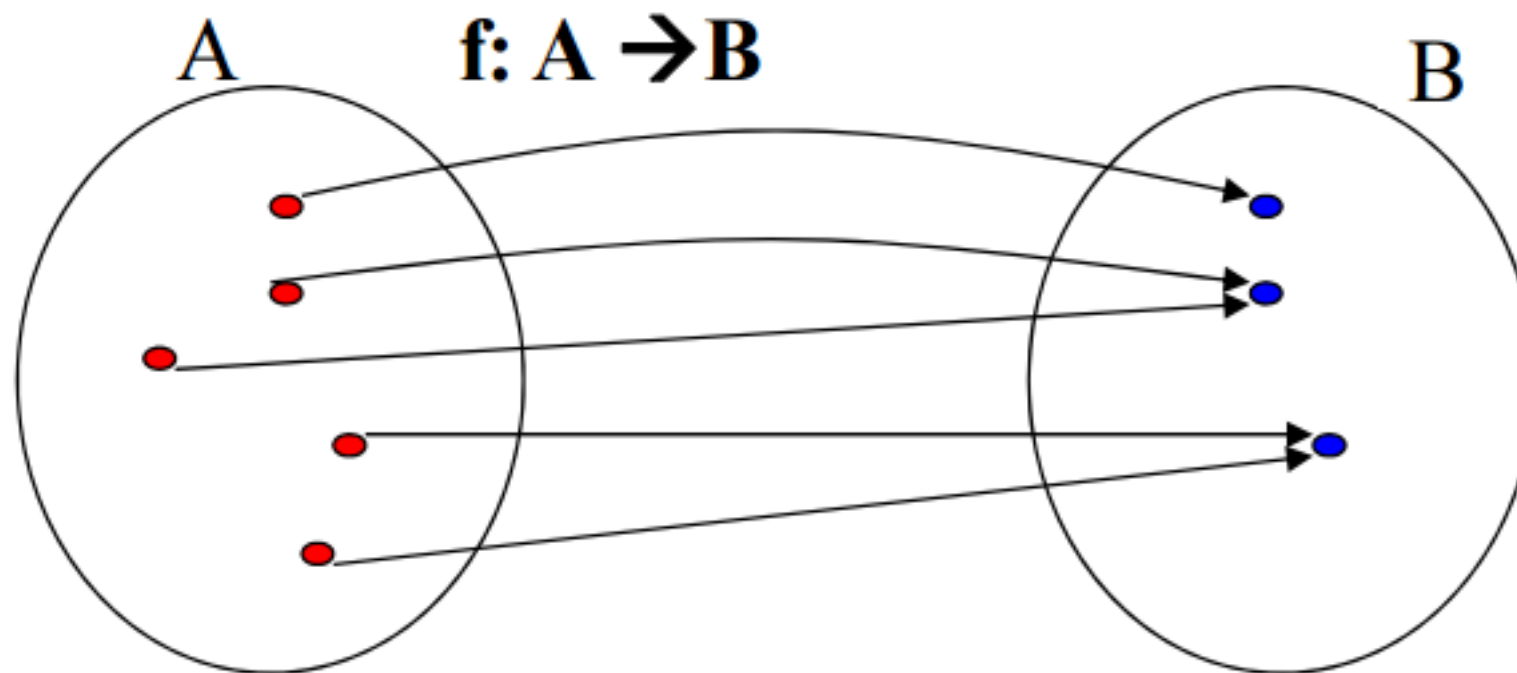
Surjective Functions

○ Examples:

- Let *f : {1, 2, 3} → {a, b, c}*, where *1 ↦ c, 2 ↦ a, 3 ↦ c*. Is *f* onto?
  No

- Let *g : **Z** → **Z***, where *g(x) = 2x − 1.* Is *g* surjective?
  No

- Let *h : {1, 2, 3, 4} → {0, 1, 2}*, where *h(x) = x mod 3*. Is *h* onto?
  Yes

SUSTech

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 subjective.

- also known as a one-to-one correspondence
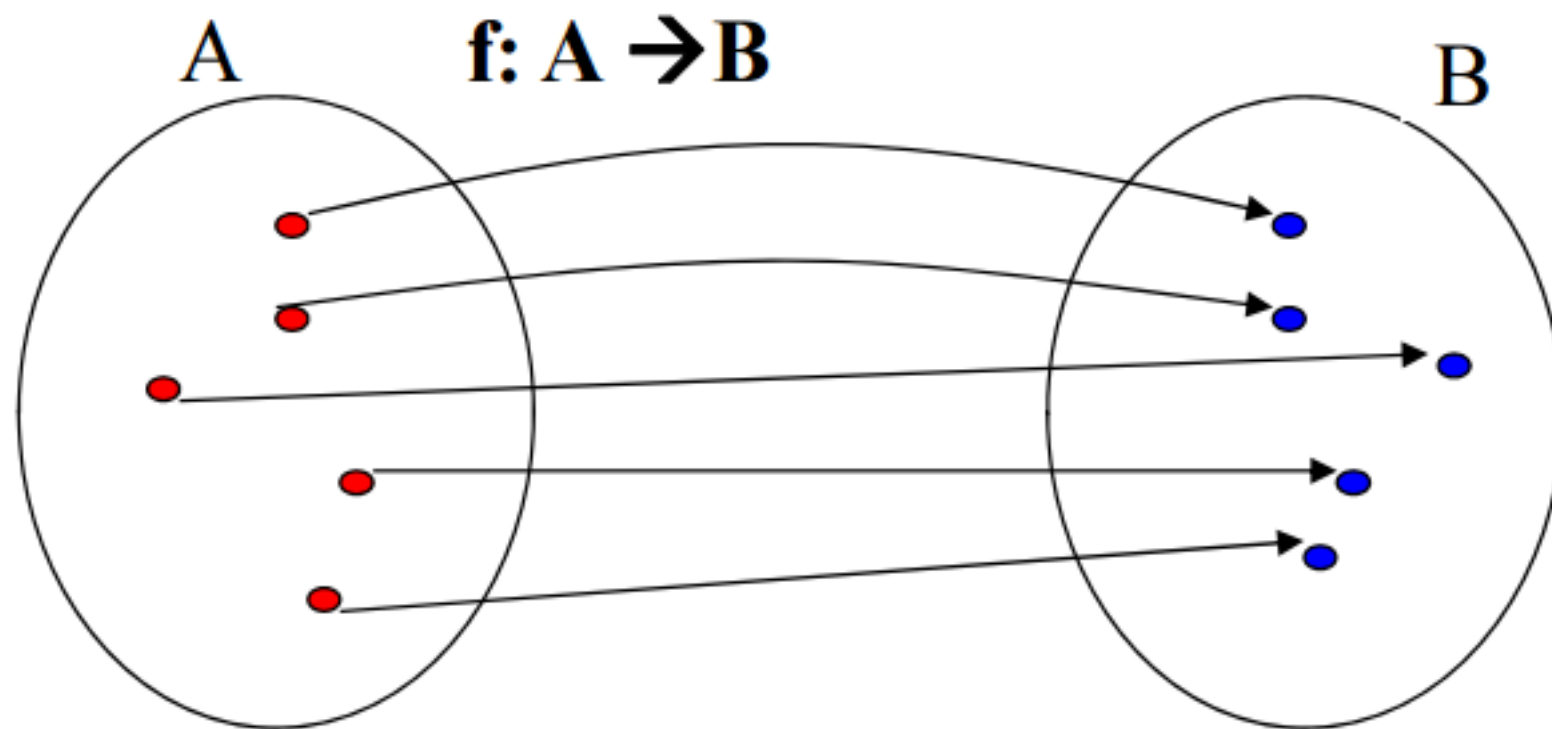
Bijective Functions

○ Examples:

- Let *f : {1, 2, 3} → {a, b, c}*, where *1 ↦ c, 2 ↦ a, 3 ↦ b*. Is *f* bijective?
  Yes

- Let *g : N → N*, where $g(x) = \lfloor x/2 \rfloor$ (floor function). Is *g* bijective?
  No (not injective)

Summary

○ 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)*

- Prove that "for a function $f : A \to B$ with $|A| = |B| = n$, f is one-to-one if and only if f is onto." *Hint: how do we 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

Note

○ "For a function $f : A \rightarrow A$, f is one-to-one if and only if f is onto."
 what about this? is it still true?

○ This is false when A is an infinite set. Here is a counterexample:

- $f : N \rightarrow N$, where $f(x) = 2x$. It is easy to see that f is one-to-one but not onto, e.g., 1 has not preimage.

SUSTech

Sum/Product of Real-Valued Functions

- Let f_1 and f_2 be functions from A to $\mathbf{R}$. Then $f_1 + f_2$ and $f_1 f_2$ are also functions form A to $\mathbf{R}$ defined for all $x \in A$ by

  - $(f_1 + f_2)(x) = f_1(x) + f_2(x)$

  - $(f_1 f_2)(x) = f_1(x) f_2(x)$

- Example: $f_1 = x - 1$, $f_2 = x^3 + 1$

  - $(f_1 + f_2)(x) = x^3 + x$

  - $(f_1 f_2)(x) = x^4 - x^3 + x - 1$

SUSTech

Inverse Functions

○ Let *f : A → B* be a bijection. The inverse of *f* is the function that assigns to *b* ∈ *B* the unique element *a* ∈ *A* such that *f(a) = b*, denoted by *f $^{-1}$*. Hence, *f $^{-1}$(b) = a w*hen *f(a) = b*. In this case, *f* is called invertible.
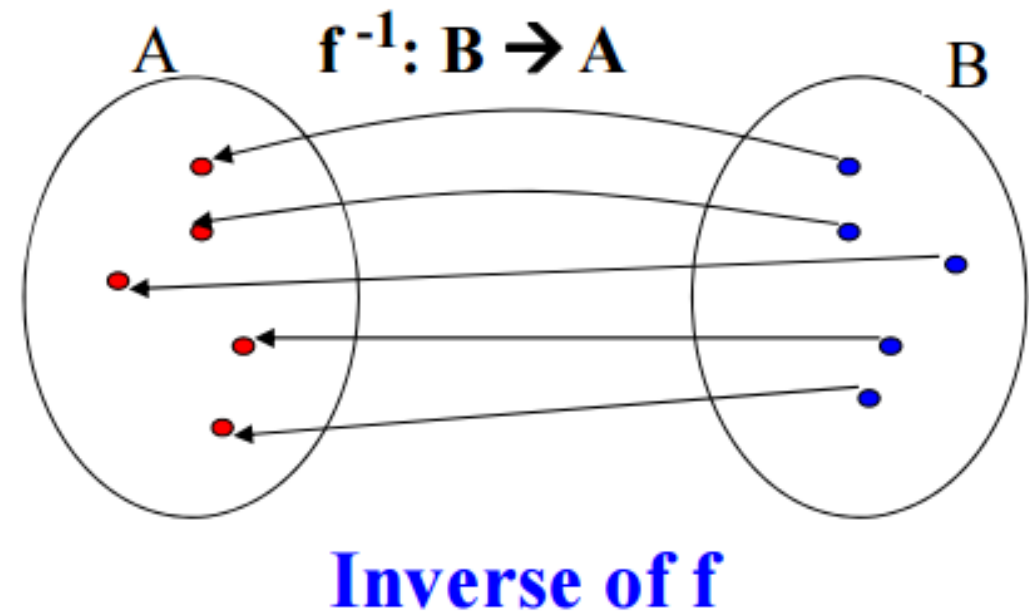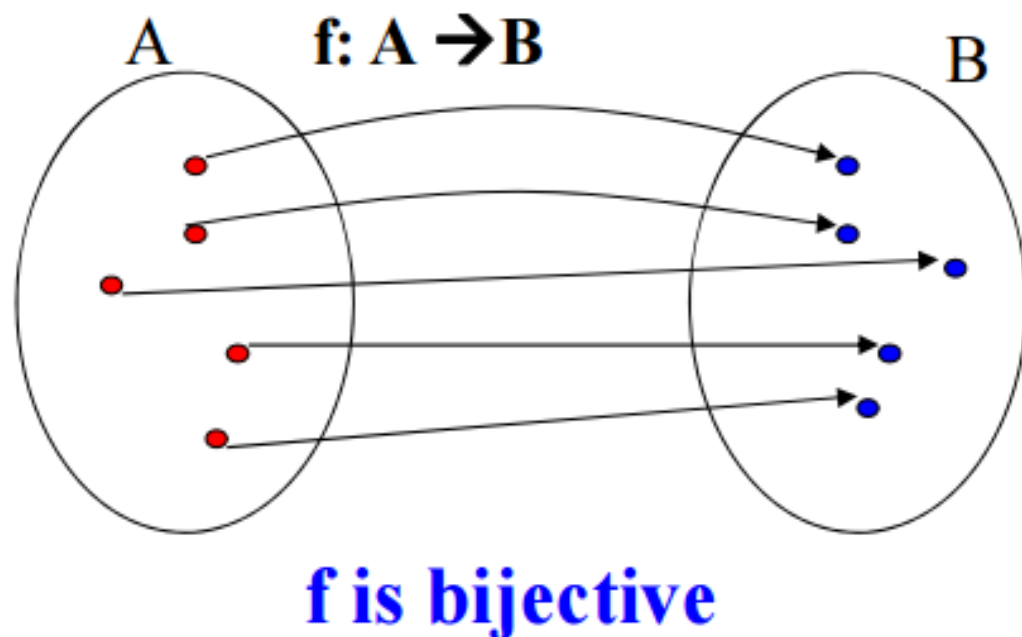
f is bijective

Inverse of f

Inverse Functions

○ Prove that: "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*
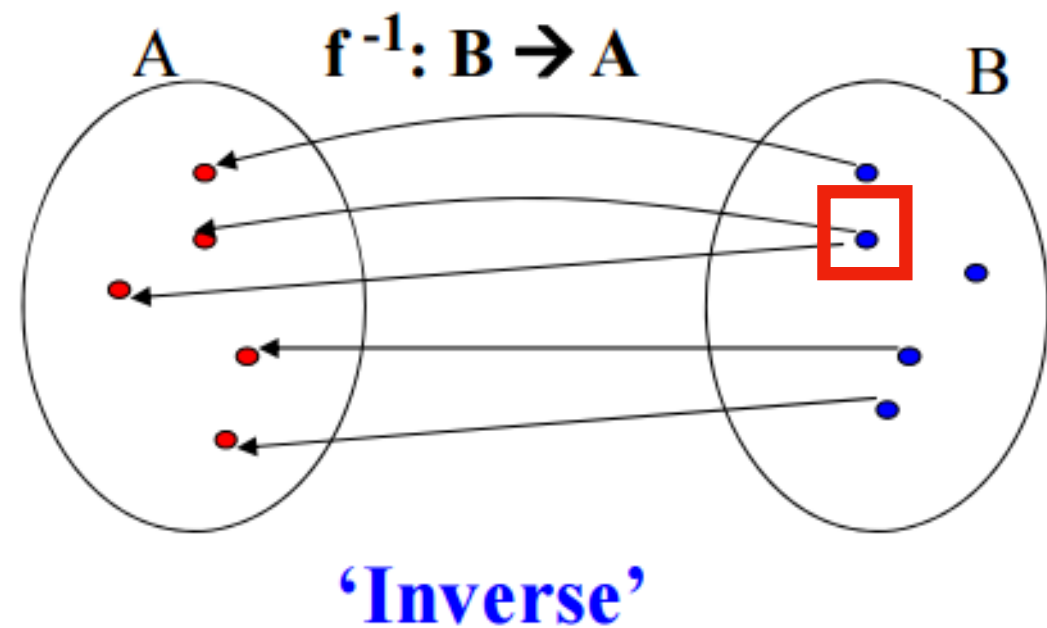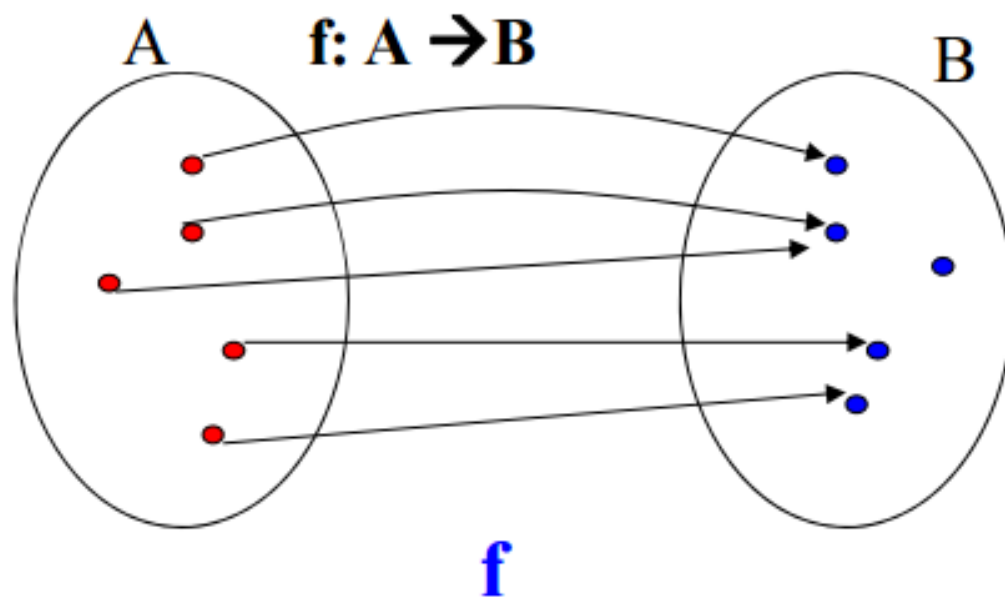
Inverse Functions

○ Prove that: "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
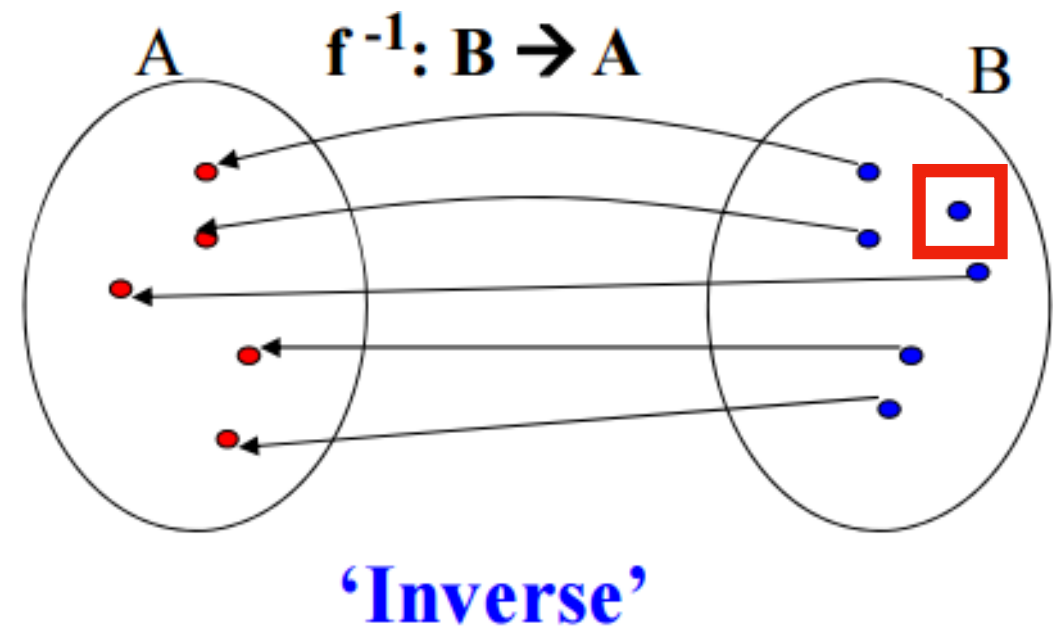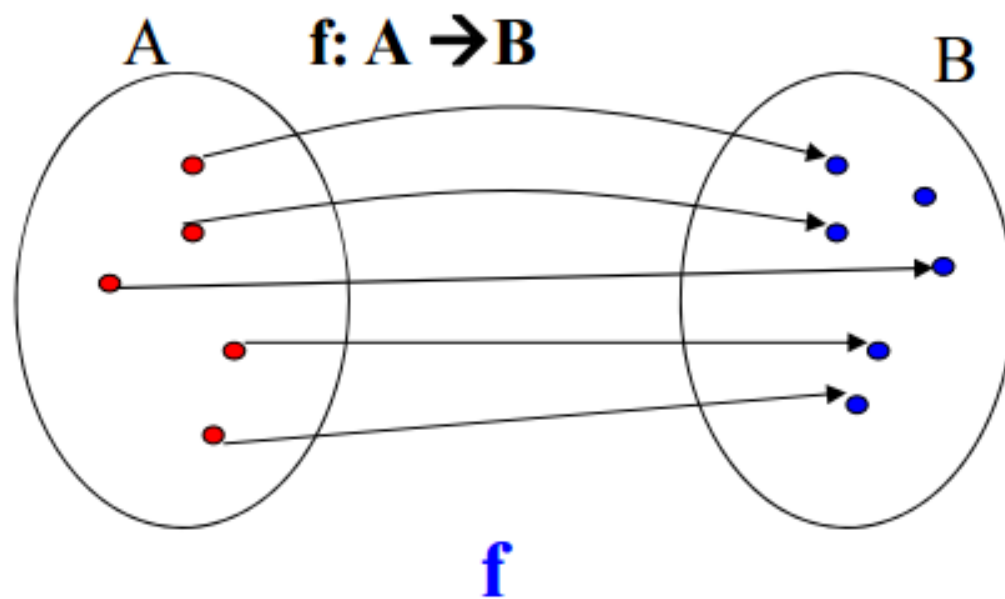
Inverse Functions

○ Example 1:

- $f : \mathbf{R} \to \mathbf{R}$, where $f(x) = 2x - 1$

- What is the inverse function f^{-1}?

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

○ Example 2:

- $f : \mathbf{Z} \to \mathbf{Z}$, where $f(x) = 2x - 1$

- Is f invertible?

  No, because f is not onto, e.g., 0 has no preimage.

SUSTech

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 by $(f \circ g)(x) = f(g(x))$.
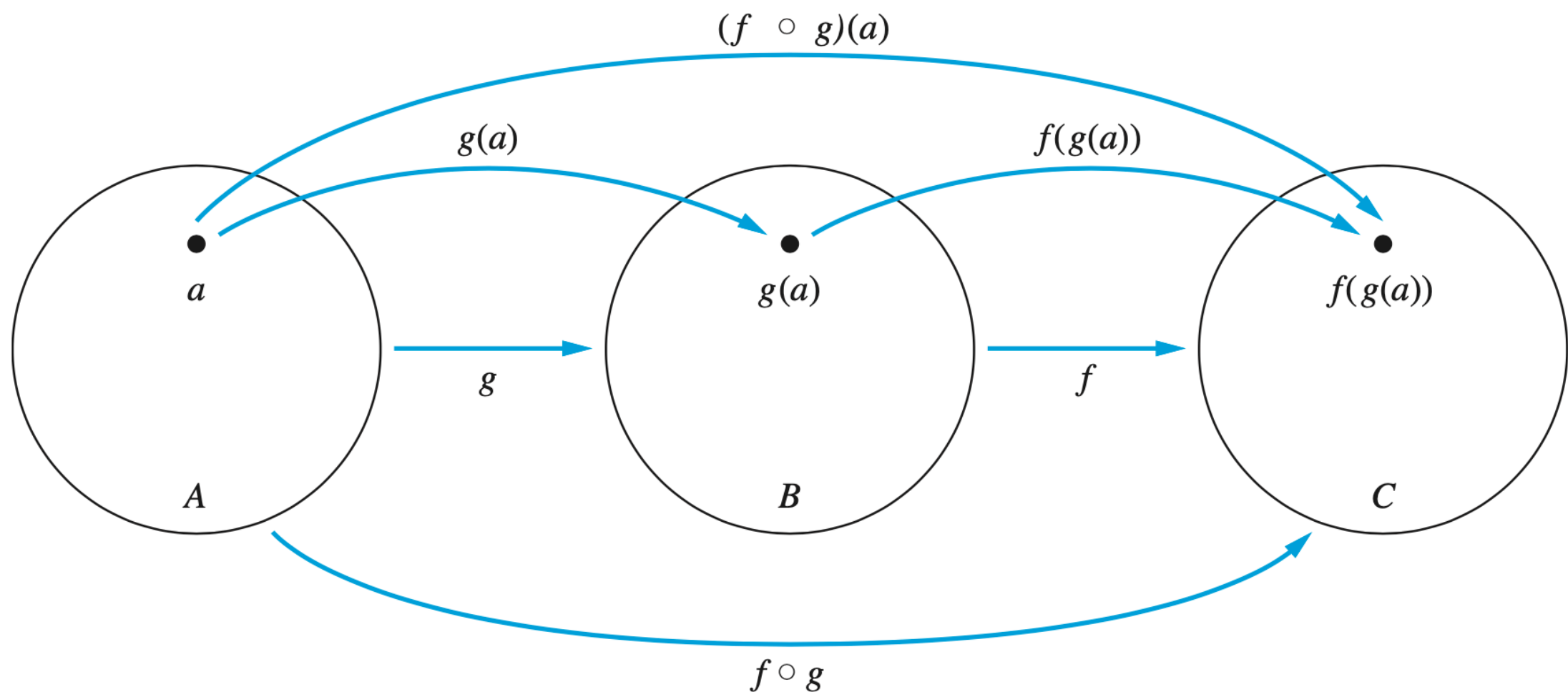
Composition of Functions

○ Example 1: (*A = {1, 2, 3}* and *B = {a, b, c, d})*

- *f : A → B where 1 ↦ b, 2 ↦ a, 3 ↦ d*

- *g : A → A where 1 ↦ 3, 2 ↦ 1, 3 ↦ 2*

- What is *f ○ g*?
  f ○ g : A → B where 1 ↦ d, 2 ↦ b, 3 ↦ a

○ Example 2:

- *f : **Z** → **Z** where f(x) = 2x*

- *g : **Z** → **Z** where g(x) = x^2*

- What are *f ○ g* and *g ○ f*?
  (f ○ g)(x) = 2x^2   *(g ○ f)(x) = 4x^2*   * order of composition matters*

SUSTech

Composition of Functions

○ Suppose that f is a bijection from A to B and let I_A and I_B denote the identity functions on the sets A and B, respectively. 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) $\lceil x + n \rceil = \lceil x \rceil + n$

SUSTech

Exercise *(3 mins)*

○ Prove that: "if x is a real number, then $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + 1/2 \rfloor$."

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

SUSTech

Sequences and Summations

Sequences

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

$$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \ldots$$

$$a_1 \quad a_2 \quad a_3 \quad a_4 \quad a_5 \quad a_6 \ldots$$

$$\{a_n\}$$
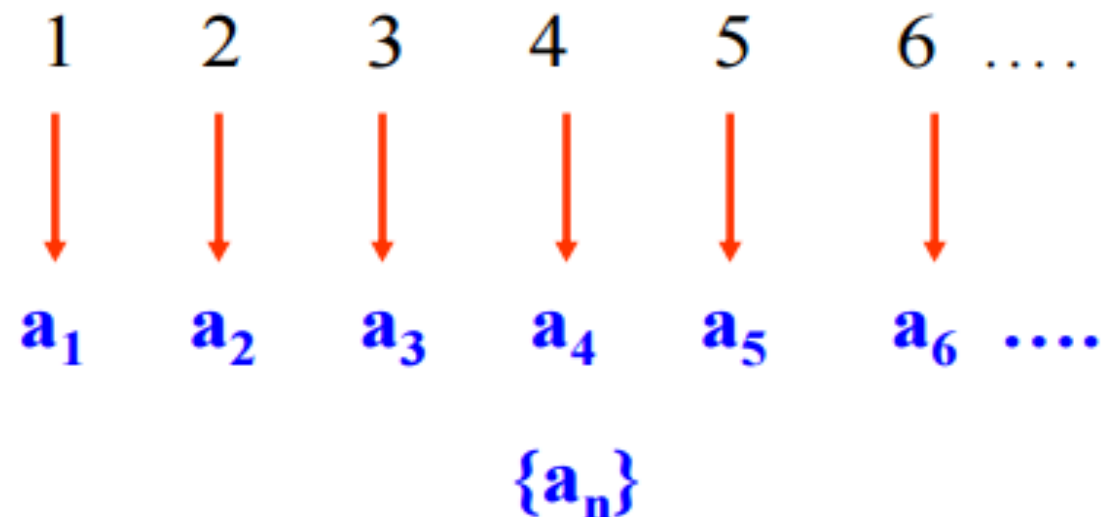
○ Notations:

- 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

Sequences

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

$$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad \dots$$

$$a_1 \quad a_2 \quad a_3 \quad a_4 \quad a_5 \quad a_6 \quad \dots$$

$$\{a_n\}$$
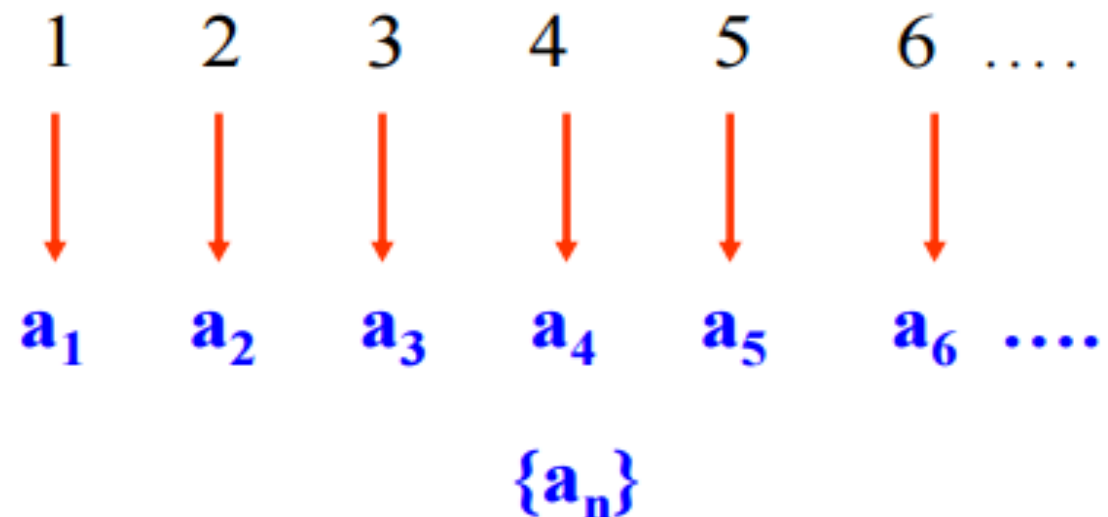
○ Examples:

- $a_n = n^2$, where $n = 1, 2, 3, \dots$

- $a_n = (-1)^n$, where $n = 0, 1, 2, \dots$

- $a_n = 2^n$, where $n = 0, 1, 2, \dots$

SUSTech

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 $n = 0, 1, 2, 3, \ldots$

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

SUSTech

Recursively Defined Sequences

○ The n-th element a_n of the sequence $\{a_n\}$ is defined recursively in terms of the previous elements of the sequence and the initial elements of the sequence.

○ 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 $f_0 = 0$, $f_0 = 1$ (Fibonacci sequence)

SUSTech

Summations

- The summation of the 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:

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

SUSTech

Summations

- The sum of the first *n + 1* terms 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 of the first *n + 1* terms 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?

SUSTech

Summations

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

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

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

Exterior *(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

Infinite Series

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

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

- Differentiating the above formula on both sides:

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

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

Proof without calculus:

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

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

$S_n = (1 - x^n)/(1 - x)^2 - nx^n/(1 - x) \to 1/(1-x)^2$ when $n \to \infty$

SUSTech

Useful Summation Formulas

TABLE 2 Some Useful Summation Formulae.	
Sum	*Closed Form*
$\displaystyle\sum_{k=0}^{n} ar^k \ (r \neq 0)$	$\dfrac{ar^{n+1} - a}{r - 1}, r \neq 1$
$\displaystyle\sum_{k=1}^{n} k$	$\dfrac{n(n+1)}{2}$
$\displaystyle\sum_{k=1}^{n} k^2$	$\dfrac{n(n+1)(2n+1)}{6}$
$\displaystyle\sum_{k=1}^{n} k^3$	$\dfrac{n^2(n+1)^2}{4}$
$\displaystyle\sum_{k=0}^{\infty} x^k, \ |x| < 1$	$\dfrac{1}{1-x}$
$\displaystyle\sum_{k=1}^{\infty} kx^{k-1}, \ |x| < 1$	$\dfrac{1}{(1-x)^2}$

Cardinality of Infinite Sets

Cardinality of Sets

○ Recall that the cardinality of a finite set is defined by the number of the elements in the set.

○ The sets A and B have the same cardinality if there is a one-to-one correspondence (bijection) between elements in A and B.

- Cardinality of infinite sets may be counter-intuitive, e.g., $|\mathbf{N}| = |\mathbf{Z}|$.

○ If there is a one-to-one function from A to B, the cardinality of A is less than or equal to the cardinality of B, denoted by $|A| \leq |B|$. Moreover, when $|A| \leq |B|$ and A and B have different cardinalities, we say that the cardinality of A is less than the cardinality of B, denoted by $|A| < |B|$.

SUSTech

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 one-to-one functions $f : A \rightarrow B$ and $g : B \rightarrow A$, then there exists a one-to-one correspondence between *A* and *B*. Note that sets *A* and *B* can be infinite.

- *the proof is quite subtle and please refer to the textbook for details*

○ Example of its application:

- Show that $|(0, 1)| = |(0, 1]|$.

- Proof: Construct two one-to-one functions:

  $f : (0, 1) \rightarrow (0, 1], f(x) = x$

  $g : (0, 1] \rightarrow (0, 1), g(x) = x/2$

Countable and Uncountable Sets

○ A set that either is finite or has the same cardinality as the set of positive integers Z^+ is called countable, otherwise, it is called uncountable.

- A countable set S can be infinite, but there must exist a bijection between Z^+ and S.

- Intuitively, the cardinality of a countable set is less than that of any uncountable set. (The formal proof requires 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.

SUSTech

Hilbert's Grand Hotel

○ The Grand Hotel has countably infinite number of rooms, each occupied by a guest. We can always accommodate a new guest at this hotel. This seems impossible because all rooms are already occupied. How is this possible?
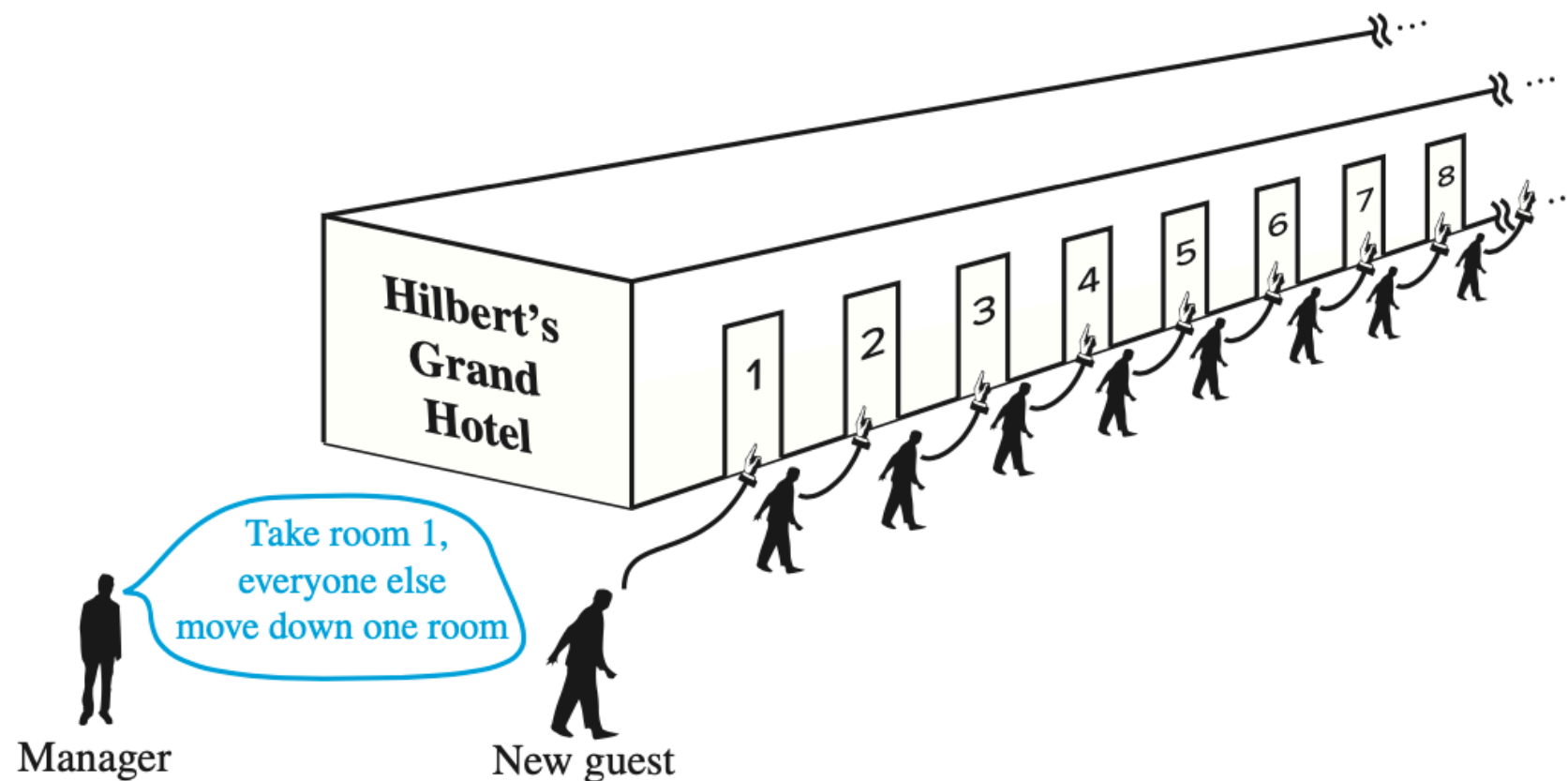
Countable Sets

○ Example: *A = {0, 2, 4, 6, …} - Is this set countable?*

- (By definition) Is there a bijection *f : $\mathbf{Z}^+ \to A$*?

- Define a function *f : $x \mapsto 2x - 2$*. This is a bijection!

- Proof:

  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 $\mathbf{Z}^+$

SUSTech

Countable Sets

○ **Theorem:** "The set of integers **Z** is countable."

○ Proof:

- **Directly:** list a sequence: *0, 1, −1, 2, −2, 3, −3, …*

- **Alternatively:** define a bijection from **Z**+ to **Z**:

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

    when *n* is odd: *f(n) = −(n−1)/2*

SUSTech

Countable Sets

○ **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*

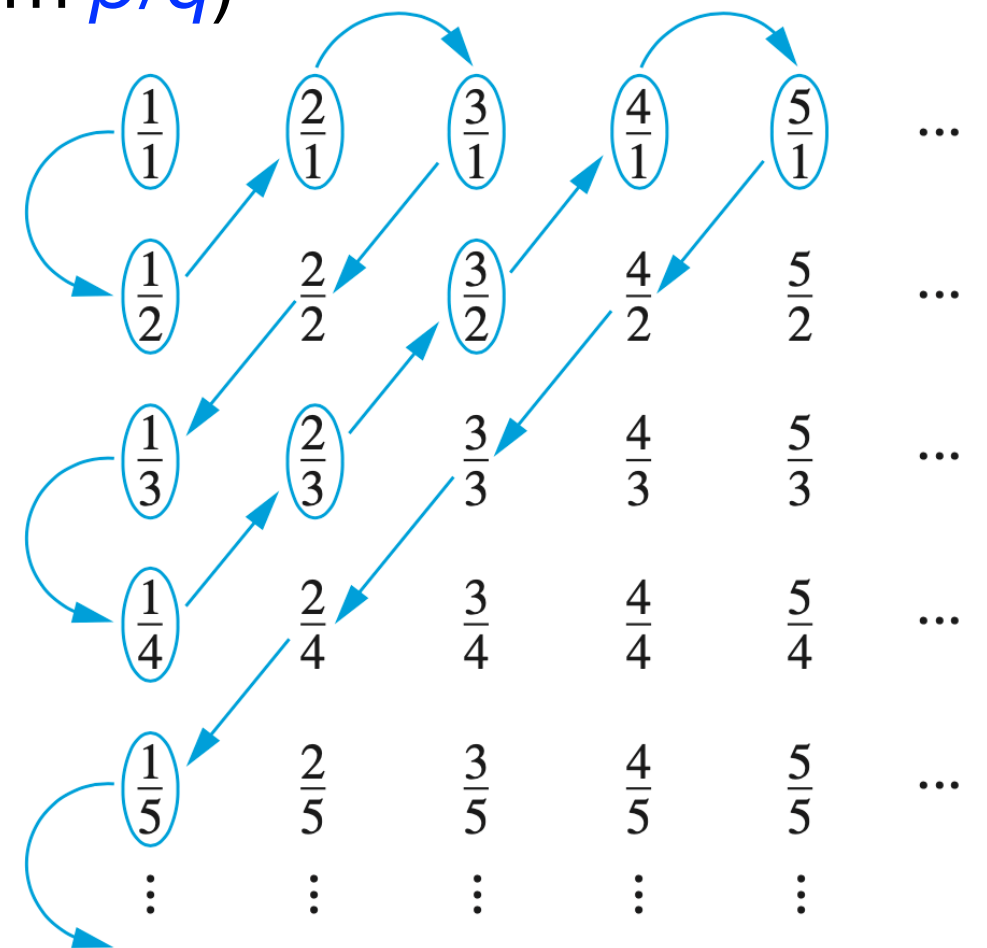   *3/1, ~~2/2,~~ 1/3*

  …

- 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

○ **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 Z^+ to S.

Exercise *(2 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 Z^+ to *S*.

Uncountable Sets

- **Theorem:** "The set of real numbers **R** is uncountable."

- Proof by contradiction:

  - Assume that **R** is countable.
    Then every subset of **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

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

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

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

    …

    with $d_{ij} \in \{0, 1, 2, \ldots, 9\}$ *Note that 1 = 0.999999···*

  - Construct a real number *r* that is not included in the above list:

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

SUSTech

Uncountable Sets

○ **Theorem:** "The set of real numbers **R** is uncountable."

○ Proof by contradiction: (Cantor's diagonalization argument)

- Assume that **R** is countable.
  Then every subset of **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

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

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

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

  …

  with $d_{ij} \in \{0, 1, 2, \ldots, 9\}$ *Note that 1 = 0.999999…*

- Construct a real number *r* that is not included in the above list:

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

SUSTech

Exercise *(3 mins)*

○ **Theorem:** "The set $\mathcal{P}(\boldsymbol{N})$ is uncountable."

Recall that $\mathcal{P}(\boldsymbol{N})$ contains all subsets of $\boldsymbol{N}$

○ **Theorem:** "The set of real numbers $\boldsymbol{R}$ is uncountable."

○ Proof by contradiction: (Cantor's diagonalization 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

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

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

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

  …

  with $d_{ij} \in \{0, 1, 2, \ldots, 9\}$ *Note that 1 = 0.999999⋯*

- Construct a real number *r* that is not included in the above list:

  $r = 0.d_1 d_2 d_3 d_4 \cdots$ *where* $d_i \neq \boldsymbol{d_{ii}}$

SUSTech

Computable vs Uncomputable

○ 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 any particular programming language is countable.

- **Part 2:** The set of functions from Z^+ to *{0, 1, …, 9}* is uncountable.

- Conclusion: there exists a function $f^* : Z^+ \rightarrow$ *{0, 1, …, 9}* that does not correspond to any computer program, i.e., uncomputable.

SUSTech

The Continuum Hypothesis

○ We know that $|N| < |\mathcal{P}(N)|$

- because N is countable but $\mathcal{P}(N)$ is uncountable

- **Cantor's theorem:** $|S| < |\mathcal{P}(S)|$ holds for any set S

○ **Question:** Is there a set A such that $|N| < |A| < |\mathcal{P}(N)|$?

○ **Continuum Hypothesis:** the above set A does not exist

- this is a very important open problem in mathematics

SUSTech

04 Complexity of Algorithms

To be continued…

Quiz Requirements

○ Quiz 1 will take place in class on Oct 17th and it captures materials from 01 Introduction to 03 Sets and Functions.

○ We will have 2 quizzes in total for this course:

- 3~6 questions in 30 minutes for each quiz

- bring several pieces of paper to write your answers on

- submit your answers as a single file via Blackboard

- must attend the quiz in person

SUSTech