

Discrete Mathematics for Computer Science

Lecture 4: Set and Function

Dr. Ming Tang

Department of Computer Science and Engineering
Southern University of Science and Technology (SUSTech)
Email: tangm3@sustech.edu.cn

Questions from Students

Prove that $\sqrt{2}$ is **irrational**. (Rational numbers are those of the form $\frac{m}{n}$, where m and n are integers.)

Proof: Suppose that $\sqrt{2}$ is rational. Then, there exist integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors.

Since $\sqrt{2} = a/b$, it follows that $2b^2 = a^2$. By the definition of an even integer, it follows that a^2 is even, so a is even.

Since a is even, $a = 2k$ for some integer k . Thus, $b^2 = 2k^2$. This implies that b^2 is even, so b is even.

As a result, a and b have a common factor 2, which contradicts our assumption.

Questions from Students

- Write the numbers $1, 2, 3, \dots, 2n$ on a blackboard, where n is an odd integer.
- Pick any two of the numbers, j and k , write $|j - k|$ on the board and erase j and k . Continue this process until only one integer is written on the board.

Prove that this integer must be odd.

Questions: Why is $1 + 2 + \dots + 2n$ odd?

$$1 + 2 + \dots + 2n = \frac{2n(1 + 2n)}{2} = n(1 + 2n)$$

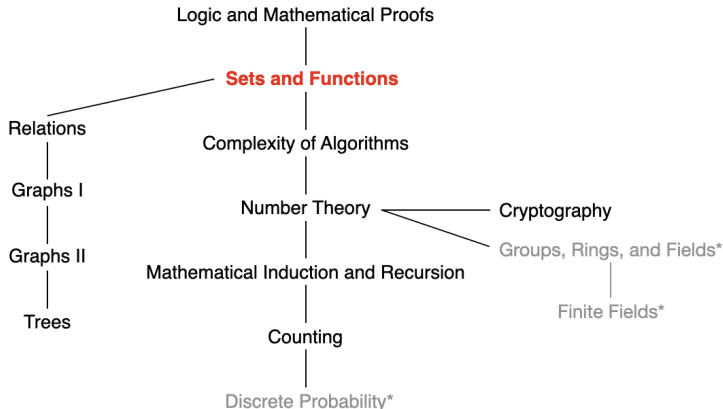
- n is odd, so $n = 2k + 1$
- $n(1 + 2n) = (2k + 1)(1 + 4k + 2) = 2(4k^2 + 5k + 1) + 1$



SUSTech

Southern University
of Science and
Technology

This Lecture



Set and Functions: set, set operations, functions, sequences and summation, cardinality of sets



SUSTech

Southern University
of Science and
Technology

Sets

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

- $A = \{1, 2, 3, 4\}$
- $B = \{a, b, c, d\}$
- $C = \{a, 2, 1, \text{Mary}\}$

Many discrete structures are built with sets:

- combinations
- relations
- graphs

Set Representation

Examples:

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

Representing a set by:

- listing (enumerating) the elements
- if enumeration is hard, use ellipses (...)
- definition by property, using the set builder

$$\{x \mid x \text{ has property } P \text{ or property } P(x)\}$$

Notation:

- $a \in A$: a is an element of set A
- $a \notin A$: a is not an element of set A

Important sets

- Natural numbers:

- ◇ $\mathbf{N} = \{0, 1, 2, 3, \dots\}$

- Integers:

- ◇ $\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

- Positive integers:

- ◇ $\mathbf{Z}^+ = \{1, 2, 3, \dots\}$

- Rational numbers:

- ◇ $\mathbf{Q} = \{\frac{p}{q} \mid p \in \mathbf{Z}, q \in \mathbf{Z}, q \neq 0\}$

- Real numbers:

- ◇ \mathbf{R}

- Complex numbers:

- ◇ \mathbf{C}

Important sets

- $[a, b] = \{x \mid a \leq x \leq b\}$
 $[a, b) = \{x \mid a \leq x < b\}$
 $(a, b] = \{x \mid a < x \leq b\}$
 $(a, b) = \{x \mid a < x < b\}$
- Two sets A, B are *equal* if and only if $\forall x (x \in A \leftrightarrow x \in B)$.

Are sets $\{1, 2, 5\}$ and $\{2, 5, 1\}$ equal? **Yes**

Are sets $\{1, 2, 2, 2, 5\}$ and $\{2, 5, 1\}$ equal? **Yes**

Universal and Empty Set

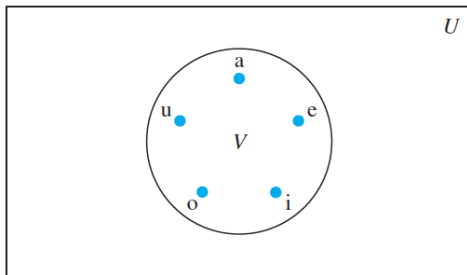
The **universal set** is the set of all objects under consideration, denoted by U .

The **empty set** is the set of no object, denoted by \emptyset or $\{\}$.

- Are \emptyset and $\{\emptyset\}$ equal? **No**

Venn Diagrams

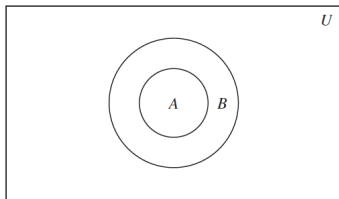
A set can be visualized using Venn diagrams



Subset

The set A is a **subset** of B **if and only if** every element of A is also an element of B , i.e., $\forall x(x \in A \rightarrow x \in B)$, denoted by $A \subseteq B$.

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



Proof of Subset

Proof:

- Showing $A \subseteq B$: if x belongs to A , then x also belongs to B .
- Showing $A \not\subseteq B$: find a single $x \in A$ such that $x \notin B$.

Theorems

Prove that $\emptyset \subseteq S$.

Proof:

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

Prove that $S \subseteq S$.

Proof:

By definition, we need to prove $\forall x(x \in S \rightarrow x \in S)$. This is **obviously true**.

Note: two sets are equal if and only if each is a subset of the other:

$$\forall x(x \in A \leftrightarrow x \in B)$$

The Size of a Set – 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 is said to be infinite if it is not finite.

Examples:

- $A = \{1, 2, 3, \dots, 20\}$, where $|A| = 20$
- $B = \{1, 2, 3, \dots\}$, which is infinite
- $|\emptyset| = 0$
- $|\{\emptyset\}| = 1$

Power Set

Many problems involve testing all combinations of elements of a set to see if they satisfy some property. To consider all such combinations,

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

Example: What is the power set of the set $\{0, 1, 2\}$?

$$\mathcal{P}(\{0, 1, 2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}$$

If S is a set with $|S| = n$, then $|\mathcal{P}(S)| = 2^n$. Why?

Power Set

What is the power set of \emptyset ?

$$\mathcal{P}(\emptyset) = \{\emptyset\}.$$

What is the power set of the set $\{\emptyset\}$?

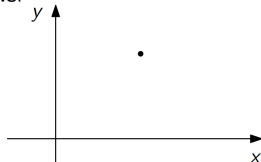
$$\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}.$$

Tuples

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

Ordered 2-tuples are called **ordered pairs**

Example:



coordinates of a point in the 2-D plane

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

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** ordered pairs (a, b) , where $a \in A$ and $b \in B$:

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

Example:

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

Are $A \times B$ and $B \times A$ equal? **No**, $A \times B \neq B \times A$

What is the cardinality $|A \times B|$? $|A \times B| = |A| \times |B|$

Cartesian Product

The Cartesian product of the sets A_1, A_2, \dots, A_n , denoted by $A_1 \times A_2 \times \dots \times A_n$, is the set of ordered n -tuples (a_1, a_2, \dots, a_n) where $a_i \in A_i$ for $i = 1, \dots, n$:

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

Example:

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

$$A \times B \times C =$$

$$\{(0, 1, 0), (0, 1, 1), (0, 1, 2), (0, 2, 0), (0, 2, 1), (0, 2, 2), \\ (1, 1, 0), (1, 1, 1), (1, 1, 2), (1, 2, 0), (1, 2, 1), (1, 2, 2)\}$$

Let A be a set. A^n denotes $A \times A \times \dots \times A$ with n sets:

$$A^n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A \text{ for } i = 1, 2, \dots, n\}$$



SUSTech

Southern University
of Science and
Technology

Relation

A **subset** R of the Cartesian product $A \times B$ is called a **relation** from the set A to the set B .

Example: What are the ordered pairs in the less than or equal to relation, which contains (a, b) if $a \leq b$, on the set $\{0, 1, 2, 3\}$?

The ordered pair (a, b) belongs to R if and only if both a and b belong to $\{0, 1, 2, 3\}$ and $a \leq b$. Consequently,

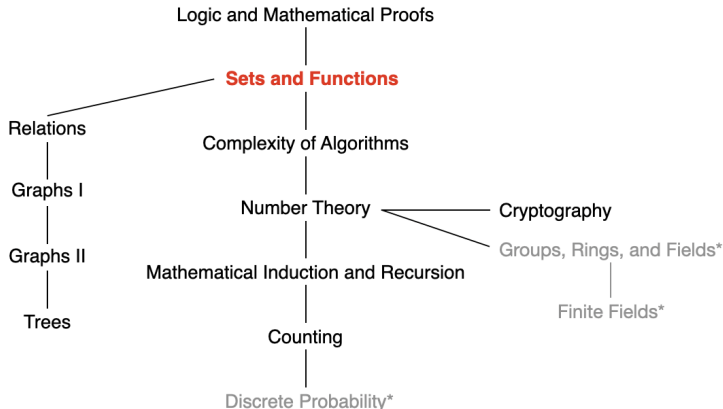
$$R = \{(0, 0), (0, 1), (0, 2), (0, 3), (1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$$

.

Summary of Set

- Set: unordered collection of objects
- Subset $A \subseteq B$
- Cardinality: size of set
- Power of set $\mathcal{P}(A)$
- Tuple: (a, b)
- Cartesian Product $A \times B$
- Relation: a subset of $A \times B$

This Lecture



Set and Functions: set, set operations, functions, sequences and summation, cardinality of sets

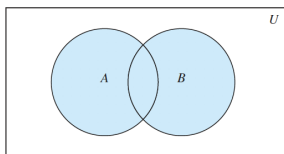


SUSTech

Southern University
of Science and
Technology

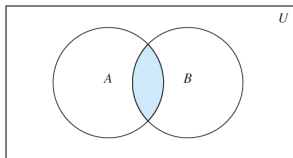
Set Operations

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



$A \cup B$ is shaded.

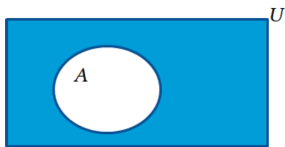
Intersection: The intersection of the sets A and B , denoted by $A \cap B$, is the set $\{x \mid x \in A \wedge x \in B\}$.



$A \cap B$ is shaded.

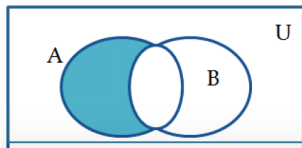
Set Operations

Complement: If A is a set, then the complement of the set A (with respect to U), denoted by \bar{A} is the set $U - A$, $\bar{A} = \{x \in U \mid x \notin A\}$



Difference: Let A and B be sets. The difference of A and B , denoted by $A - B$, is the set containing the elements of A that are not in B .

$$A - B = \{x \mid x \in A \wedge x \notin B\} = A \cap \bar{B}.$$



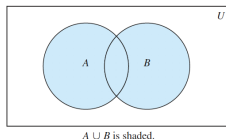
Disjoint Sets

Two sets A and B are called **disjoint** if their intersection is empty, i.e., $A \cap B = \emptyset$.

Example: $A = \{1, 3, 5, 7\}$ and $B = \{2, 4, 6\}$ are disjoint, because $A \cap B = \emptyset$.

Cardinality of the Union

What is the cardinality of $A \cup B$?



$$|A \cup B| = |A| + |B| - |A \cap B|$$

The generalization of this result to unions of an arbitrary number of sets is called the **principle of inclusion–exclusion**

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

THE PRINCIPLE OF INCLUSION–EXCLUSION Let A_1, A_2, \dots, A_n be finite sets. Then

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| = & \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\ & + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \dots + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n|. \end{aligned}$$

Shen University
Science and
Technology

Exercises

■ $U = \{0, 1, 2, \dots, 10\}, A = \{1, 2, 3, 4, 5\}, B = \{4, 5, 6, 7, 8\}$

1. $A \cup B$

2. $A \cap B$

3. \bar{A}

4. \bar{B}

5. $A - B$

6. $B - A$

■ $U = \{0, 1, 2, \dots, 10\}, A = \{1, 2, 3, 4, 5\}, B = \{4, 5, 6, 7, 8\}$

1. $A \cup B$ $\{1, 2, 3, 4, 5, 6, 7, 8\}$

Set Identities

The properties and laws of sets that help us demonstrate and prove set operations, subsets and equivalence.

■ Identity laws

- ◇ $A \cup \emptyset = A$
- ◇ $A \cap U = A$

■ Domination laws

- ◇ $A \cup U = U$
- ◇ $A \cap \emptyset = \emptyset$

■ Idempotent laws

- ◇ $A \cup A = A$
- ◇ $A \cap A = A$

■ Complementation laws

- ◇ $\overline{\overline{A}} = A$

Set Identities

■ Commutative laws

$$\diamond A \cup B = B \cup A$$

$$\diamond A \cap B = B \cap A$$

■ Associative laws

$$\diamond A \cup (B \cup C) = (A \cup B) \cup C$$

$$\diamond A \cap (B \cap C) = (A \cap B) \cap C$$

■ Distributive laws

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

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

■ De Morgan's laws

$$\diamond \overline{A \cap B} = \bar{A} \cup \bar{B}$$

$$\diamond \overline{A \cup B} = \bar{A} \cap \bar{B}$$

Set Identities

■ Absorbion laws

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

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

■ Complement laws

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

$$\diamond A \cap \bar{A} = \emptyset$$

Proof of Set Identities

Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Proof 1: Using membership tables. Consider an arbitrary element x : 1, x is in A ; 0, x is not in A .

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

Proof 2: by showing that $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$ and $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$

• $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$:

- ▶ Suppose that $x \in \overline{A \cap B}$. By the definition of complement, $x \notin A \cap B$. Using the definition of intersection, $\neg((x \in A) \wedge (x \in B))$ is true.
- ▶ By applying De Morgan's law, $\neg(x \in A) \vee \neg(x \in B)$. Thus, $x \notin A$ or $x \notin B$. Using the definition of the complement of a set, $x \in \bar{A}$ or $x \in \bar{B}$.
- ▶ By the definition of union, we see that $x \in \bar{A} \cup \bar{B}$. Thus, $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$.

• $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$

Proof of Set Identities

Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Proof 1: using membership tables.

Proof 2: by showing that $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$ and $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$

Proof 3: Using set builder and logical equivalences

$\overline{A \cap B} = \{x \mid x \notin A \cap B\}$	by definition of complement
$= \{x \mid \neg(x \in (A \cap B))\}$	by definition of does not belong symbol
$= \{x \mid \neg(x \in A \wedge x \in B)\}$	by definition of intersection
$= \{x \mid \neg(x \in A) \vee \neg(x \in B)\}$	by the first De Morgan law for logical equivalences
$= \{x \mid x \notin A \vee x \notin B\}$	by definition of does not belong symbol
$= \{x \mid x \in \bar{A} \vee x \in \bar{B}\}$	by definition of complement
$= \{x \mid x \in \bar{A} \cup \bar{B}\}$	by definition of union
$= \bar{A} \cup \bar{B}$	by meaning of set builder notation



Generalized Unions and Intersections

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

Computer Representation of Sets

Question: How to represent sets in a computer?

- One solution: explicitly store the elements in a list
 - ▶ Computing the union, intersection, or difference operations would be **time-consuming**, because of the needs for searching elements.
- A better solution: 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.
 - ▶ Universal set U is finite and with n elements
 - ▶ Represent a subset A of U with n bits, where the i -th bit is 1 if a_i belongs to A and is 0 if a_i does not belong to A .

Computer Representation of Sets

Example: $U = \{1, 2, 3, 4, 5\}$

$A = \{2, 5\}$. Thus, A is represented by 01001

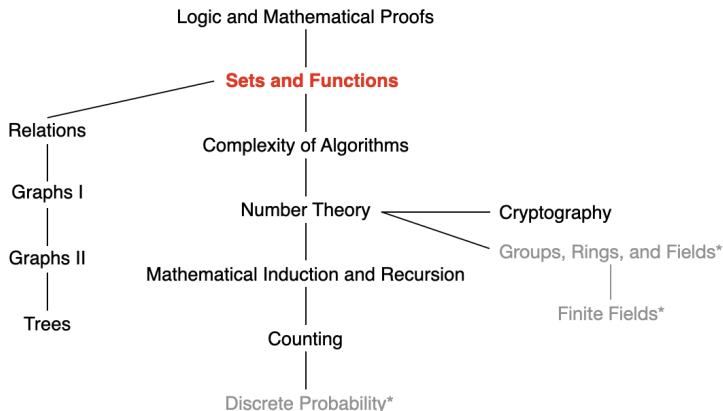
$B = \{1, 5\}$. Thus, B is represented by 10001

- Union: $A \vee B = 11001$, i.e., $\{1, 2, 5\}$
- Intersection: $A \wedge B = 00001$, i.e., $\{5\}$
- Complement: $\bar{A} = 10110$, i.e., $\{1, 3, 4\}$

Summary of Set Operations

- Union $A \cup B$, cardinality (principle of inclusion-exclusion)
- Intersection $A \cap B$
- Complement \bar{A}
- Difference $A - B$
- Disjoint set
- Set identities
- Proof of set identities
 - ▶ membership table, subset, set build and logical equivalences
- Computer representations

This Lecture



Set and Functions: set, set operations, functions, sequences and summation, cardinality of sets



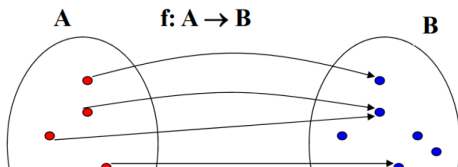
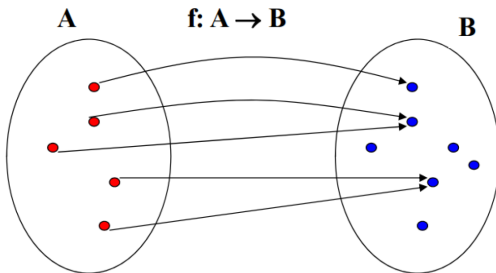
SUSTech

Southern University
of Science and
Technology

Function

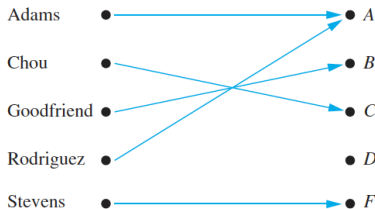
Let A and B be two sets. A **function** from A to B , denoted by $f: A \rightarrow B$, is an assignment of **exactly one** element of B to **each** element of A .

- We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a of A .



Representing Functions

- 1 Explicitly state the assignments between elements of the two sets



Note: $\text{Admas} \mapsto A$, $\text{Chou} \mapsto C$, ...

- 2 By a formula: $f(x) = x + 1$
- 3 By a relation from A to B : (Abdul, 22), (Brenda, 24), (Carla, 21), (Desire, 22), (Eddie, 24), and (Felicia, 22).

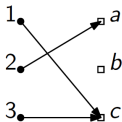
Important Sets of Functions

Let f be a function from A to B .

- A is the **domain** of f ; 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:

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



Example:

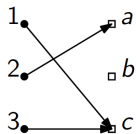
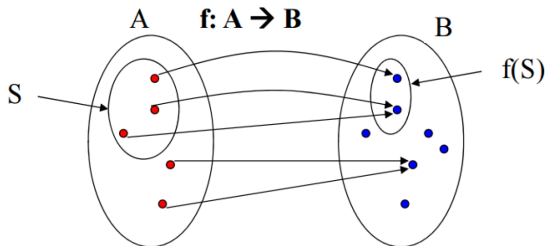
$$A = \{1, 2, 3\}, B = \{a, b, c\}$$

– c is the **image** of 1



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 the elements of S , denoted by $f(S)$, where $f(S) = \{f(s) | s \in S\}$



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

One-to-One and Onto Functions

- **One-to-one function**

- ▶ never assign the same value to two different domain elements.

- **Onto function**

- ▶ every member of the codomain is the image of some element of the domain.

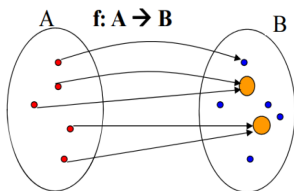
- **One-to-one correspondence**

- ▶ One-to-one and onto

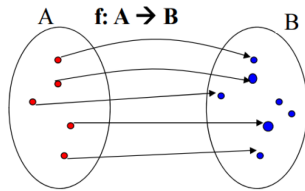
One-to-One (Injective) Function

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 . Also called an **injection**.

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



Not injective



Injective function

How about:

- $f(x) \neq f(y)$ implies $x \neq y$?
- $x = y$ implies $f(x) = f(y)$?

One-to-One (Injective) Function

Example 1:

Whether the function f from $\{a, b, c, d\}$ to $\{1, 2, 3, 4, 5\}$ with $f(a) = 4$, $f(b) = 5$, $f(c) = 1$, and $f(d) = 3$ is one-to-one? **Yes.**

Example 2:

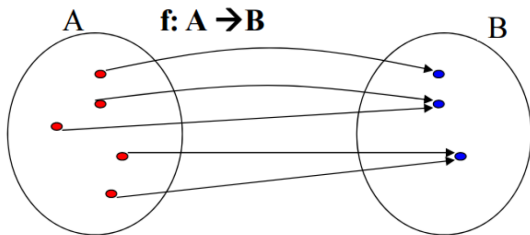
Whether the function $f(x) = x^2$ from the set of integers to the set of integers is one-to-one? **No**, $f(-1) = f(1)$

What if it is from the set of **positive** integers to the set of integers? **Yes.**

Onto (Surjective) Function

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 $f(a) = b$. Also called a **surjection**.

Alternatively: A function is onto if and only if all codomain elements are covered, i.e., $f(A) = B$.



SUSTech

Southern University
of Science and
Technology

Onto (Surjective) Function: Example

Example 1:

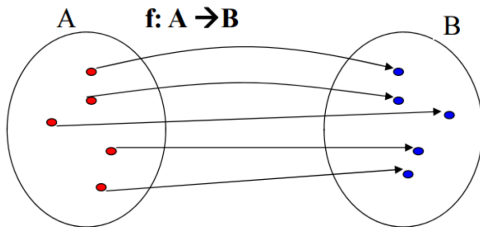
Let f be the function from $\{a, b, c, d\}$ to $\{1, 2, 3\}$ defined by $f(a) = 3$, $f(b) = 2$, $f(c) = 1$, and $f(d) = 3$. Is f an onto function? **Yes.**

What if the codomain were $\{1, 2, 3, 4\}$? **No.**

Example 2: Is the function $f(x) = x^2$ from the set of integers to the set of integers onto? **No**, as there is no integer x with $x^2 = -1$.

One-to-One Correspondence (Bijective Function)

A function f is called **one-to-one correspondence** or **bijective**, if and only if it is **both** one-to-one and onto. Also called **bijection**.



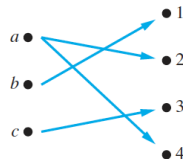
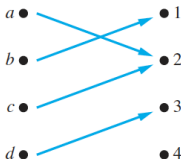
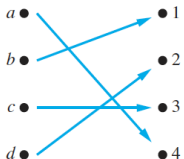
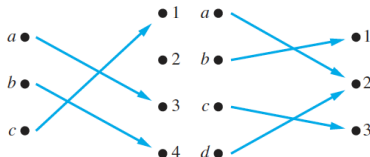
One-to-One Correspondence: Example

Example 1:

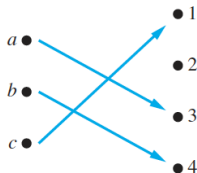
Let f be the function from $\{a, b, c, d\}$ to $\{1, 2, 3, 4\}$ with $f(a) = 4$, $f(b) = 2$, $f(c) = 1$, and $f(d) = 3$. Is f a one-to-one correspondence? **Yes.**

Example 2: Consider an identity function on A , i.e., $\iota : A \rightarrow A$, where $\iota_A(x) = x$. Is this function a one-to-one correspondence? **Yes.**

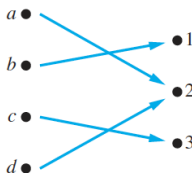
Are These Functions Injective, Surjective, Bijective?



(a) One-to-one,
not onto



(b) Onto,
not one-to-one



Proof for One-to-One and Onto

To show that f is <i>injective</i>	Show that if $f(x) = f(y)$ for all $x, y \in A$, then $x = y$
To show that f is not <i>injective</i>	Find specific elements $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$
To show that f is <i>surjective</i>	Consider an arbitrary element $y \in B$ and find an element $x \in A$ such that $f(x) = y$
To show that f is not <i>surjective</i>	Find a specific element $y \in B$ such that $f(x) \neq y$ for all $x \in A$



Example

$f : \mathbf{Z} \rightarrow \mathbf{Z}$, where $f(x) = x + 1$. Is f injective? Surjective? Bijective?

Proof:

- Injective (one-to-one function): If $f(x) = f(x')$ for any arbitrary x and x' , then $x = x'$.
- Surjective (onto function): For every integer y , there exists an integer x such that $f(x) = y$.
- Bijective (one-to-one correspondence): injective and surjective

One-to-One and Onto

Prove that “for a function $f : A \rightarrow B$ with $|A| = |B| = n$, f is one-to-one if and only if f is onto.”

Proof: Since $|A| = n$, let $\{x_1, x_2, \dots, x_n\}$ be elements of A .

- If f is one-to-one, then f is onto (direct proof): Suppose that f is one-to-one. According to the definition of one-to-one function, $f(x_i) \neq f(x_j)$ for any $i \neq j$. Thus, $|f(A)| = |\{f(x_1), \dots, f(x_n)\}| = n$. Since $|B| = n$ and $f(A) \subseteq B$, we have $f(A) = B$.
- If f is onto, then f is one-to-one (contradiction): Suppose that f is onto. Suppose that f is not one-to-one. Thus, $f(x_i) = f(x_j)$ for some $i \neq j$. Then, $|\{f(x_1), \dots, f(x_n)\}| \leq n - 1$. Note that $|f(A)| = |B| = n$, which leads to a contradiction.

One-to-One and Onto

Consider an **infinite** set A and a function from A to A . Consider the statement “For any arbitrary $f : A \rightarrow A$, f is one-to-one **if and only if** f is onto”. Is this statement true?

Proof (Counterexample): Consider the following $f : \mathbf{Z} \rightarrow \mathbf{Z}$, where $f(x) = 2x$. f is one-to-one but not onto:

- $f(1) = 2$
- $f(2) = 4$
- $f(3) = 6$
- ...

We can prove that 3 has no preimage.

Two Functions on Real Numbers

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 from 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:

$$f_1 = x - 1 \text{ and } f_2 = x^3 + 1$$

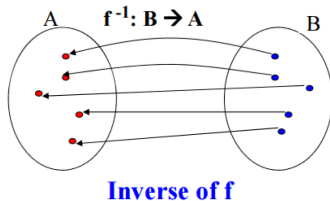
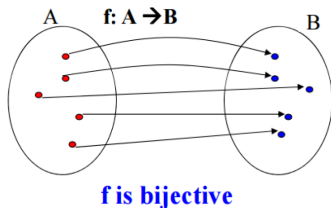
Then

$$\begin{aligned}(f_1 + f_2)(x) &= x^3 + x \\ (f_1 f_2)(x) &= x^4 - x^3 + x - 1\end{aligned}$$

Inverse Functions

Let f be a **one-to-one correspondence (bijection)** 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 $f(a) = b$.

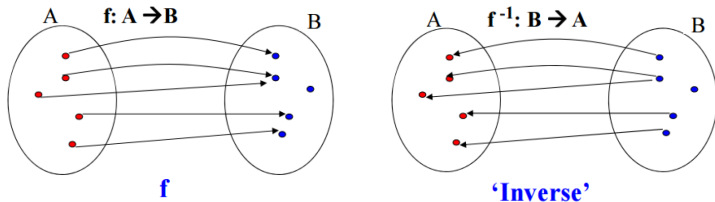


A bijection is called **invertible**.

Inverse Functions

If is **not a one-to-one correspondence (bijection)**, it is impossible to define the inverse function of f . Why?

Assume f is not one-to-one (injective):

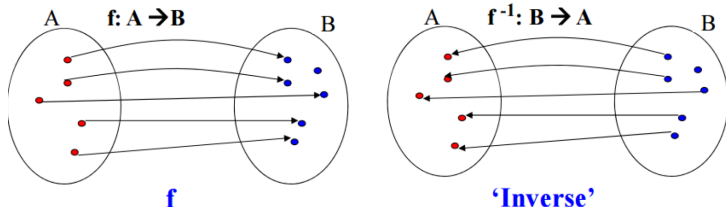


The inverse is **not a function**: one element of B is mapped to **two different** elements of A .

Inverse Functions

If is **not a one-to-one correspondence (bijection)**, it is impossible to define the inverse function of f . Why?

Assume f is not onto (surjective):



The inverse is not a function: one element of B is **not assigned** an element of A .

Proof for Inverse Function

1 Prove function f is a bijection: injective, surjective

To show that f is <i>injective</i>	Show that if $f(x) = f(y)$ for all $x, y \in A$, then $x = y$
To show that f is not <i>injective</i>	Find specific elements $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$
To show that f is <i>surjective</i>	Consider an arbitrary element $y \in B$ and find an element $x \in A$ such that $f(x) = y$
To show that f is not <i>surjective</i>	Find a specific element $y \in B$ such that $f(x) \neq y$ for all $x \in A$

2 If f is a bijection, then it is invertible

3 Determine the inverse function

Inverse Functions: Example 1

$f : \mathbf{Z} \rightarrow \mathbf{Z}$, where $f(x) = x + 1$. Is f invertible? If yes, then what is the inverse function f^{-1} ?

Proof: f is invertible, as it is a bijection (one-to-one correspondence):

- **Injective** (one-to-one function): If $f(x) = f(x')$ for any arbitrary x and x' , then $x = x'$.
- **Surjective** (onto): For every integer y , there exists an integer $x = y - 1$ such that $f(x) = y$.

To reverse the function, suppose that y is the image of x , so that $y = x + 1$. Then, $x = y - 1$. This means that $y - 1$ is the unique element of \mathbf{Z} that is sent to y by f . Consequently, $f^{-1}(y) = y - 1$.

Inverse Functions: Example 2

Let f be the function from \mathbf{R} to \mathbf{R} with $f(x) = x^2$. Is f invertible?

Proof: No, f is not invertible. This is because f is not injective, as $f(-2) = f(2)$.

What if we restrict function $f(x) = x^2$ to a function from the set of all nonnegative real numbers to the set of all nonnegative real numbers?

Proof: It is invertible, as it is a bijection:

- **Injective:** Consider x and x' . If $f(x) = f(x')$ (i.e., $x^2 = (x')^2$), then we have $x^2 - (x')^2 = (x + x')(x - x') = 0$. Since we consider the set of all nonnegative real numbers, we must have $x = x'$.
- **Surjective:** Consider an arbitrary nonnegative real number y . There exists a nonnegative real number $x = \sqrt{y}$ such that $f(x) = y$.

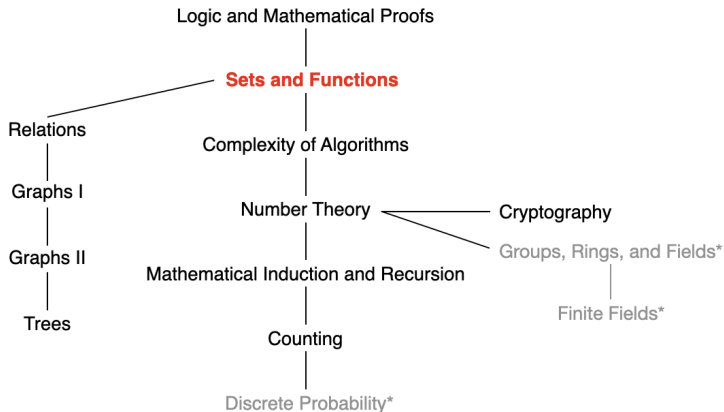
To reverse the function, suppose that y is the image of x , so that $y = x^2$. Then, $x = \sqrt{y}$. Consequently, $f^{-1}(y) = \sqrt{y}$.



Summary of Function

- Function $f : A \rightarrow B$: an assignment of **exactly one** element of B to **each** element of A
- Domain, codomain, image, preimage, range
- One-to-one function
 - ▶ also called an injection or injective function
- Onto function
 - ▶ also called a surjection or surjective function
- One-to-one correspondence
 - ▶ one-to-one and onto
 - ▶ also called a bijection or bijective function
- Inverse function
 - ▶ One-to-one correspondence

Next Lecture



Set and Functions: set, set operations, functions, sequences and summation, cardinality of sets