Department of
Computer Science and Engineering
计算机科学与工程系

CS215 DISCRETE MATH

Dr. Qi Wang
Department of Computer Science and Engineering
Office: Room413, CoE South Tower
Email: wangqi@sustech.edu.cn

Rules of Inference for Propositional Logic

- **modus ponens** (*law of detachment*) 肯定前件式

  $$(p \wedge (p \rightarrow q)) \rightarrow q$$

- **modus tollens** 否定后件式

  $$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$$

- **hypothetical syllogism** 假言三段论

  $$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$$

- **disjunctive syllogism** 选言三段论

  $$(\neg p \wedge (p \vee q)) \rightarrow q$$

Rules of Inference for Propositional Logic

- **Addition**

  $$p \to (p \vee q)$$

- **Simplication**

  $$(p \wedge q) \to p$$

- **Conjunction**

  $$((p) \wedge (q)) \to (p \wedge q)$$

- **Resolution**

  $$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$$

Rules of Inference for Quantified Statements

- **Universal Instantiation** (UI)

$$\frac{\forall x P(x)}{\therefore P(c)}$$

- **Universal Generalization** (UG)

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

- **Existential Instantiation** (EI)

$$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$$

- **Existential Generalization** (EG)

$$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$$

Methods of Proving Theorems

- Basic methods to prove theorems:
  - *direct proof*
    - $p \to q$ is proved by showing that if p is true then q follows
  - *proof by contrapositive*
    - show the contrapositive $\neg q \to \neg p$
  - *proof by contradiction*
    - show that $(p \wedge \neg q)$ contradicts the assumptions
  - *proof by cases*
    - give proofs for all possible cases
  - *proof of equivalence*
    - $p \leftrightarrow q$ is replaced with $(p \to q) \wedge (q \to p)$

Proof of Equivalences

- To prove "$p \leftrightarrow q$", show $(p \to q) \land (q \to p)$.

Example: Prove that "An integer n is odd if and only if n^2 is odd"

Proof:

◇ proof of $p \to q$: direct proof
◇ proof of $q \to p$: proof by contrapositive

Proofs with Quantifiers

- **Universally quantified statements**
  - ◇ prove the property holds for all examples
    - – proof by cases to divide the proof into different parts
  - ◇ counterexamples
    - – disprove universal statements

Proofs with Quantifiers

- **Existence proof**
  - ◇ constructive
    - – find a specific example to show the statement holds
  - ◇ nonconstructive
    - – proof by contradiction

Proof Exercises

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

Proof Exercises

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

  Proof:

  Suppose that $\sqrt{2}$ is rational. Then there exist two integers m and n such that $\gcd(m, n) = 1$ and $\sqrt{2} = m/n$. We have then $m^2 = 2n^2$. It then follows that m is even. Let $m = 2k$ for some integer k. It then follows that $n^2 = 2k^2$. Hence, n is also even. This means $\gcd(m, n)$ must have a factor 2, which contradicts to the assumption that $\gcd(m, n) = 1$.

Proof Exercises

- Prove that “There are infinitely many prime numbers ”.

- Prove that "There are infinitely many prime numbers".

Proof:

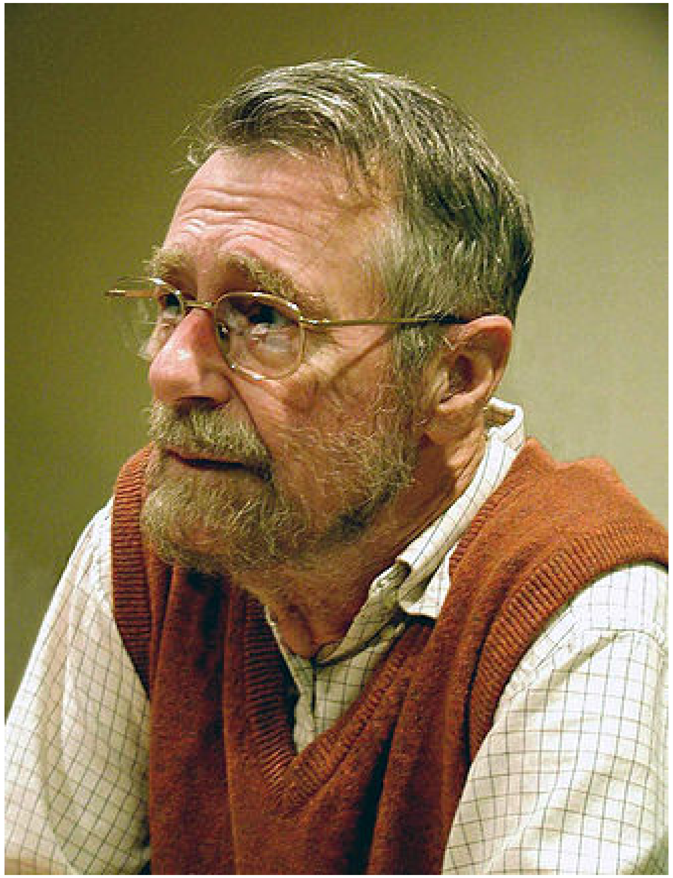
Suppose that there are only a finite number of primes. Then some prime number p is the largest of all the prime numbers, and we can list the prime numbers in ascending order:

$$2, 3, 5, 7, 11, \dots, p.$$

Let $n = (2 \times 3 \times 5 \times \cdots \times p) + 1$. Then $n > 1$, and n cannot be divided by any prime number in the list above. This means that n is also a prime. Clearly, n is larger than all the primes in the list above. This is contrary to the assumption that all primes are in the list.

Words from Dijkstra

Edsger W. Dijkstra
(1930–2002)



–"... mathematical logic is and must be the basis for software design. ... mathematical analysis of designs and specifications have become central activities in computer science research..."

Sets

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

Sets

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

- Many discrete structures are built with sets:
  - combinations
  - relations
  - graphs

Sets

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

- Many discrete structures are built with sets:
  - combinations
  - relations
  - graphs

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

Sets

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

- **Representing a set by**:
  - listing (enumerating) the elements
  - if enumeration is hard, use ellipses $(\ldots)$
  - definition by property, using the set builder

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

Important sets

- Natural numbers:
  - $\mathbf{N} = \{0, 1, 2, 3, \ldots\}$
- Integers:
  - $\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- Positive integers:
  - $\mathbf{Z}^+ = \{1, 2, 3, \ldots\}$
- 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:
  - $\mathbf{C}$

Interval Notation and Equality

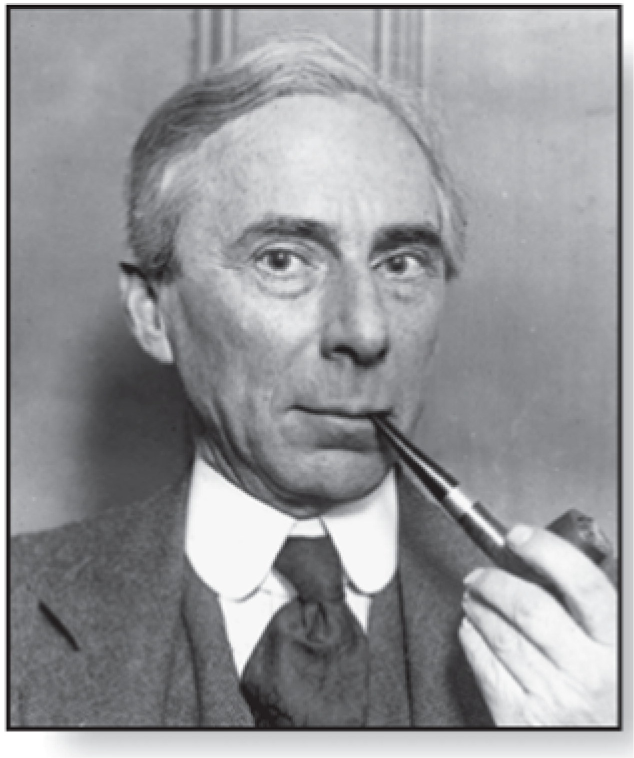
- $[a, b] = \{x \mid a \leq x \leq b\}$
  $[a, b) = \{x \mid a \leq x < b\}$
  $(a, b] = \{x \mid a < x \leq b\}$
  $(a, b) = \{x \mid a < x < b\}$

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

Russell's Paradox

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

  – Henry is a barber who shaves all people who do not shave themselves. Does Henry shave himself?



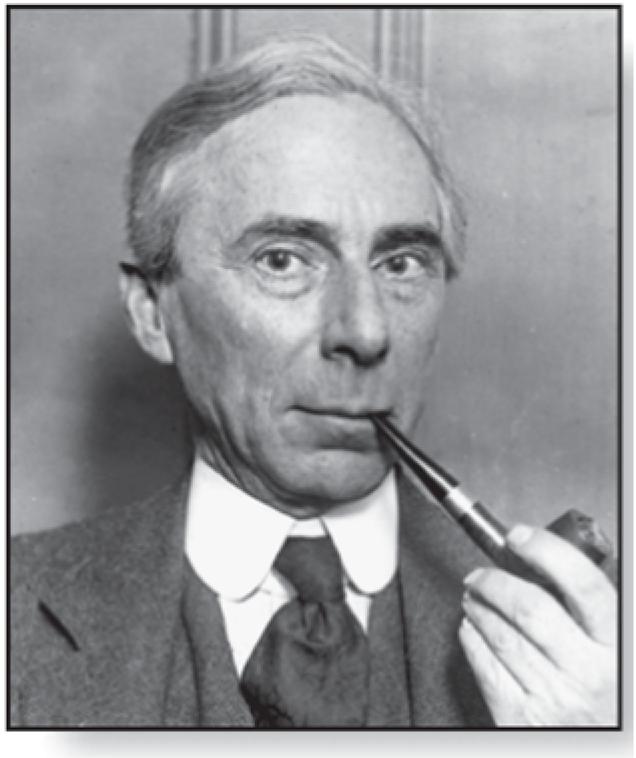
Bertrand Russell (1872-1970)
Cambridge, UK
Nobel Prize Winner

Russell's Paradox

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

  – Henry is a barber who shaves all people who do not shave themselves. Does Henry shave himself?

  Question: Is $S \in S$ or $S \notin S$?



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

Russell's Paradox

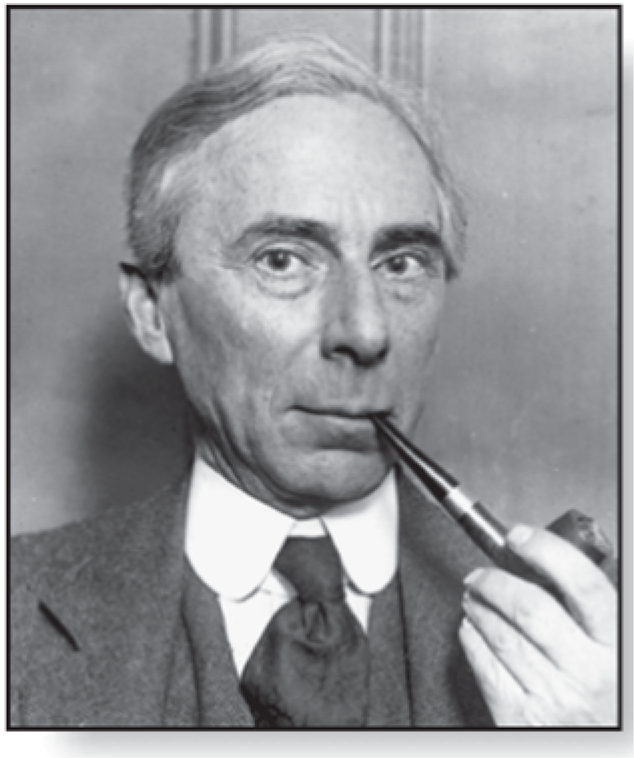
- Let $S = \{x | x \notin x\}$, is a set of sets that are not members of themselves.

  – Henry is a barber who shaves all people who do not shave themselves. Does Henry shave himself?

  Question: Is $S \in S$ or $S \notin S$?

  – $S \in S$?: S does not satisfy the condition, so $S \notin S$.

  – $S \notin S$?: S is included in the set S, so $S \in S$.



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

Russell's Paradox

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

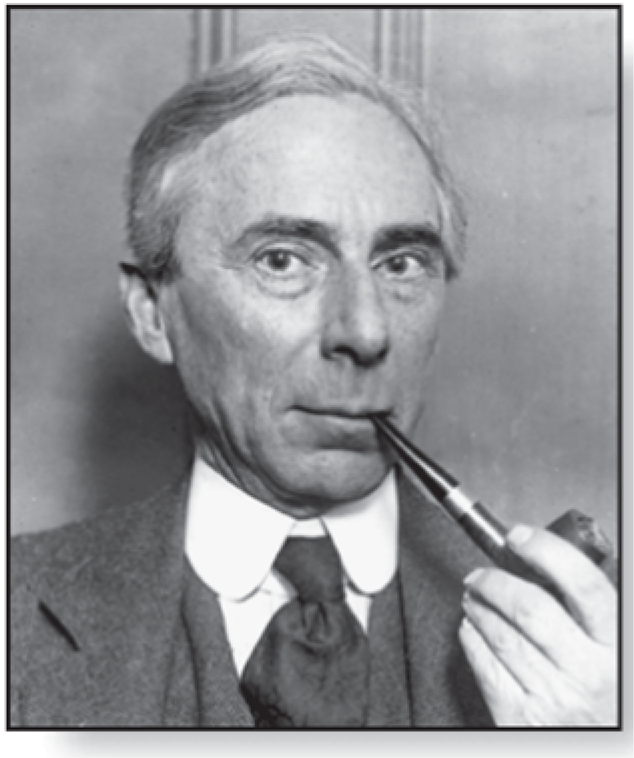
  – Henry is a barber who shaves all people who do not shave themselves. Does Henry shave himself?

  Question: Is $S \in S$ or $S \notin S$?

  – $S \in S$?: S does not satisfy the condition, so $S \notin S$.

  – $S \notin S$?: S is included in the set S, so $S \in S$.

  Answer: axiomatic set theory (out of range)



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

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 $\{\}$.

Universal and Empty Set

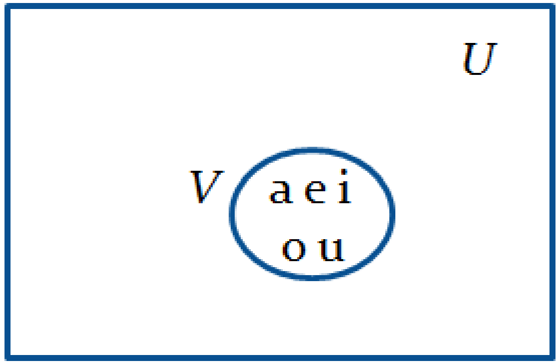
- The *universal set* is the set of all objects under consideration, denoted by U.

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

  – Note: $\emptyset \neq \{\emptyset\}$

Venn Diagrams and Subsets

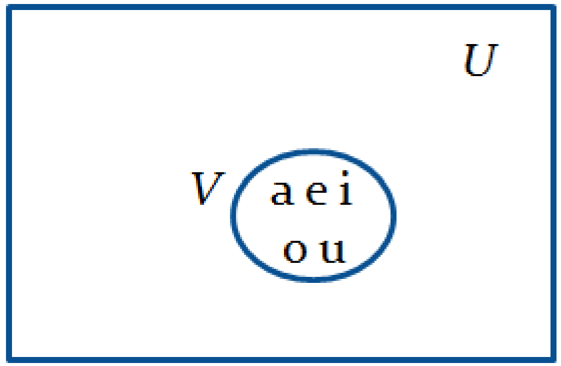
- A set can be visualized using *Venn diagrams*



John Venn (1834-1923)
Cambridge, UK

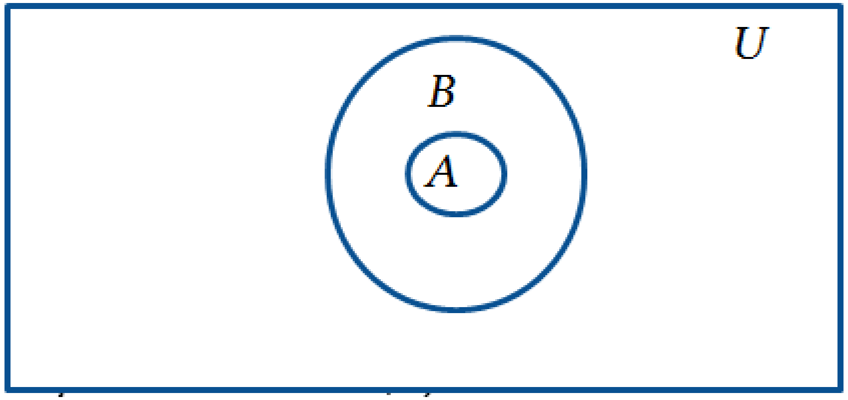
Venn Diagrams and Subsets

- A set can be visualized using *Venn diagrams*



John Venn (1834-1923)
Cambridge, UK

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



Proper Subsets and Properties

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

Proper Subsets and Properties

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

- **Theorem** $\emptyset \subseteq S$.

Proper Subsets and Properties

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

- **Theorem** $\emptyset \subseteq S$.

  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.

Subset Properties

- **Theorem** $S \subseteq S$.

Subset Properties

- **Theorem** $S \subseteq S$.

  Proof:

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

Subset Properties

- **Theorem** $S \subseteq S$.

  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.

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

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 *infinite* if it is not finite.

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 *infinite* if it is not finite.

$$A = \{1, 2, 3, \ldots, 20\} \; (|A| = 20)$$

$$B = \{1, 2, 3, \ldots\} \; (\text{infinite})$$

$$|\emptyset| = 0$$

Power Set

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

Power Set

- 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:

  - $\emptyset$
  - $\{1\}$
  - $\{1, 2\}$
  - $\{1, 2, 3\}$

  What is the power set?

Power Set

- 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:

  - $\emptyset$
  - $\{1\}$
  - $\{1, 2\}$
  - $\{1, 2, 3\}$

  What is the power set?

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

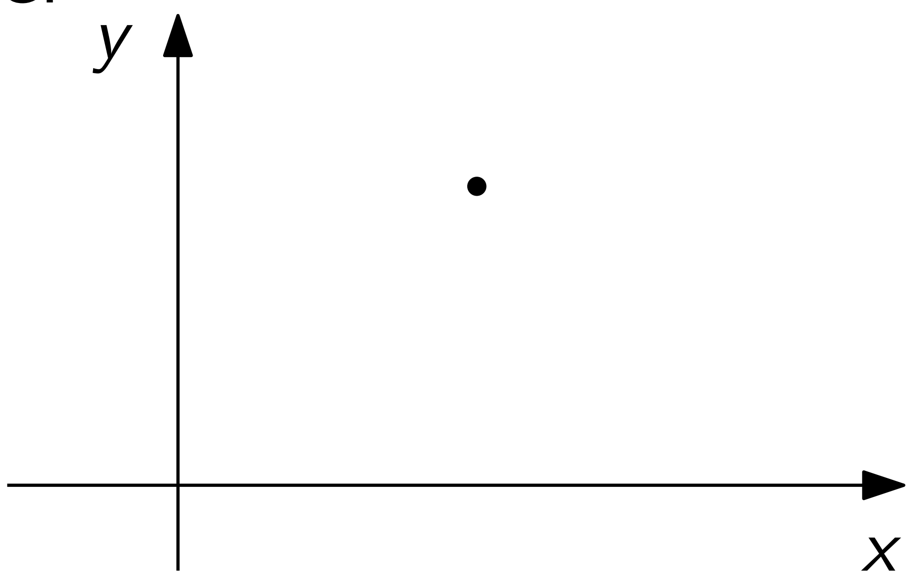
Tuples

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

Tuples

- The *ordered n-tuple* $(a_1, a_2, \ldots, a_n)$ is the ordered collection that has a_1 as its first element and 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

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 $b \in B$. Hence

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

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 $b \in B$. Hence

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

Example:

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

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

Cartesian Product

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

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

Cartesian Product

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

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

Example:

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

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

Cartesian Product

- $A \times B \neq B \times A$
- $|A \times B| = |A| \times |B|$

Cartesian Product

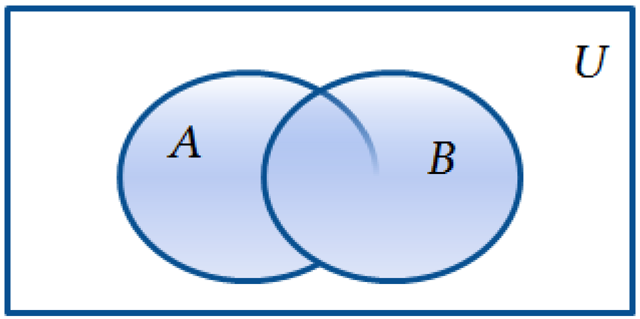
- $A \times B \neq B \times A$

- $|A \times B| = |A| \times |B|$

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

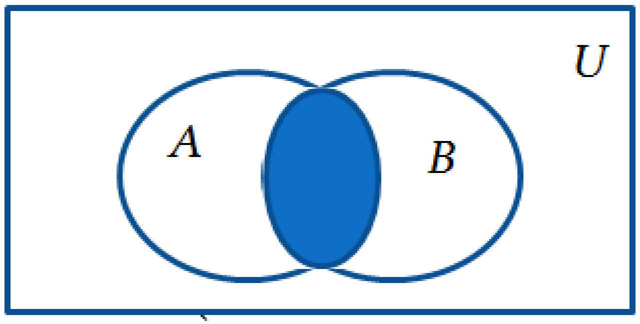
Set Operations

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



Venn Diagram for $A \cup B$

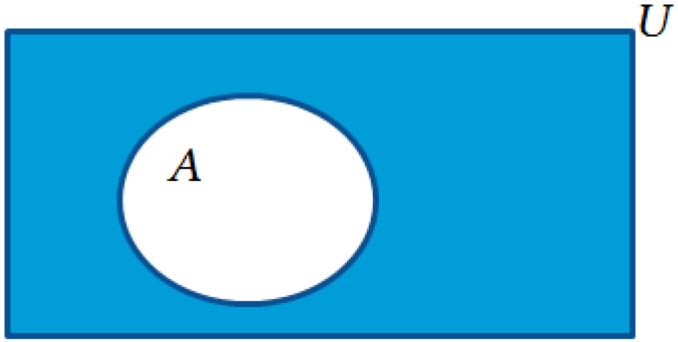
- **Intersection** The *intersection* of the sets A and B, denoted by $A \cap B$, is the set $\{x | x \in A \wedge x \in B\}$.



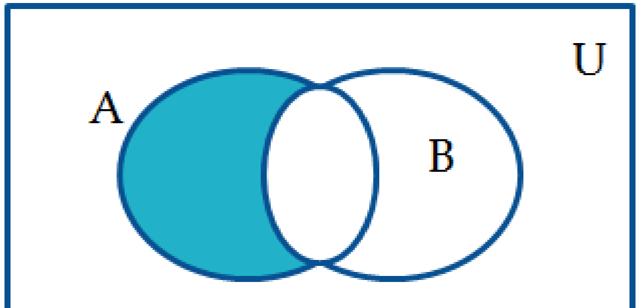
Venn Diagram for $A \cap B$

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 $U - A$, $\bar{A} = \{x \in U | x \notin A\}$.



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



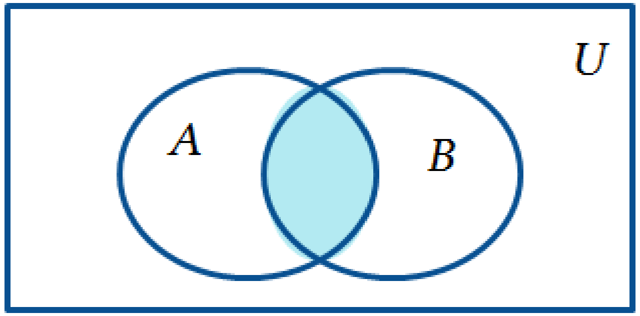
Disjoint Sets and the Cardinality of the Union

- Two sets A and B are called *disjoint* if their intersection is empty ($A \cap B = \emptyset$).

Disjoint Sets and the Cardinality of the Union

- Two sets A and B are called *disjoint* if their intersection is empty ($A \cap B = \emptyset$).

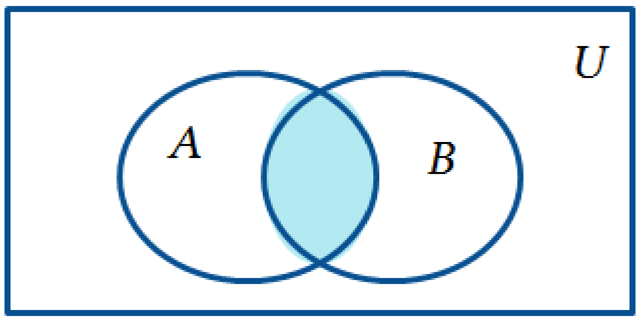
- $|A \cup B| = |A| + |B| - |A \cap B|$



Disjoint Sets and the Cardinality of the Union

- Two sets A and B are called *disjoint* if their intersection is empty ($A \cap B = \emptyset$).

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



the principle of inclusion and exclusion

Review Questions

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

1. $A \cup B$
2. $A \cap B$
3. $\bar{A}$
4. $\bar{B}$
5. $A - B$
6. $B - A$

Set Identities

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

Set Identities

- 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
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- De Morgan's laws
  - $\overline{A \cap B} = \bar{A} \cup \bar{B}$
  - $\overline{A \cup B} = \bar{A} \cap \bar{B}$

Set Identities

- Absorbtion laws
  - $A \cup (A \cap B) = A$
  - $A \cap (A \cup B) = A$
- Complement laws
  - $A \cup \bar{A} = U$
  - $A \cap \bar{A} = \emptyset$

Set Identities

- Absorbtion laws
  - $A \cup (A \cap B) = A$
  - $A \cap (A \cup B) = A$
- Complement laws
  - $A \cup \bar{A} = U$
  - $A \cap \bar{A} = \emptyset$
- Set identities can be proved using membership tables.

Set Identities

- Absorbtion laws
  - $A \cup (A \cap B) = A$
  - $A \cap (A \cup B) = A$
- Complement laws
  - $A \cup \bar{A} = U$
  - $A \cap \bar{A} = \emptyset$
- Set identities can be proved using membership tables.

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

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

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

- **Proof 2** P. 130 EXAMPLE 10

  By showing that $\forall x(x \in \overline{A \cap B} \leftrightarrow x \in \bar{A} \cup \bar{B})$

- **Proof 3**

  Using set builder and logical equivalences

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

- **Proof 2** P. 130 EXAMPLE 10

  By showing that $\forall x (x \in \overline{A \cap B} \leftrightarrow x \in \bar{A} \cup \bar{B})$

- **Proof 3** P. 131 EXAMPLE 11

  Using set builder and logical equivalences

$$
\begin{aligned}
\overline{A \cap B} &= \{x | x \notin A \cap B\} && \text{definition of complement} \\
&= \{x | \neg(x \in (A \cap B))\} && \text{definition} \\
&= \{x | \neg(x \in A \wedge x \in B)\} && \text{definition of intersection} \\
&= \{x | \neg(x \in A) \vee \neg(x \in B)\} && \text{De Morgan's laws} \\
&= \{x | x \notin A \vee x \notin B\} && \text{definition} \\
&= \{x | x \in \bar{A} \vee x \in \bar{B})\} && \text{definition of complement} \\
&= \{x | x \in \bar{A} \cup \bar{B}\} && \text{definition of union} \\
&= \bar{A} \cup \bar{B} && \text{definition}
\end{aligned}
$$

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

Computer Representation of Sets

- Question: How to represent sets in a computer?

  One solution: explicitly store the elements in a list

  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 otherwise 0.

Computer Representation of Sets

- Question: How to represent sets in a computer?

  One solution: explicitly store the elements in a list

  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 otherwise 0.

Example:

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

$A = \{2, 5\}$ – $A = 01001$
$B = \{1, 5\}$ – $B = 10001$

Computer Representation of Sets

- Question: How to represent sets in a computer?

  One solution: explicitly store the elements in a list

  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 otherwise 0.

Example:

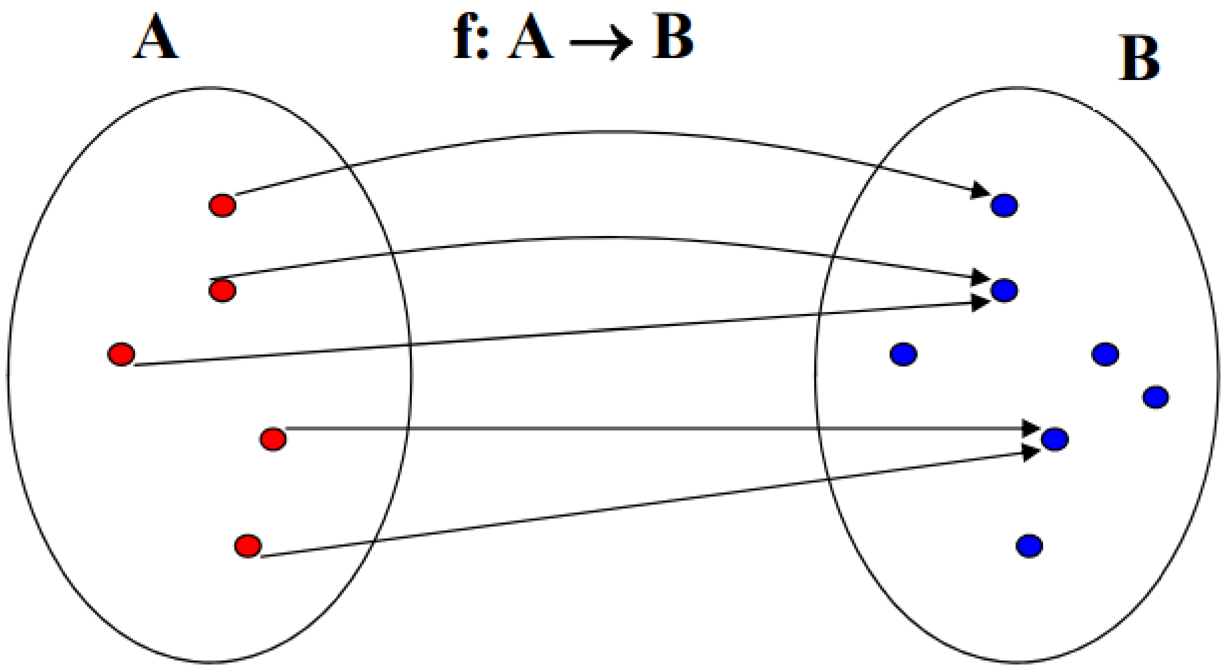
$$U = \{1, 2, 3, 4, 5\}$$

$A = \{2, 5\}$ – $A = 01001$
$B = \{1, 5\}$ – $B = 10001$

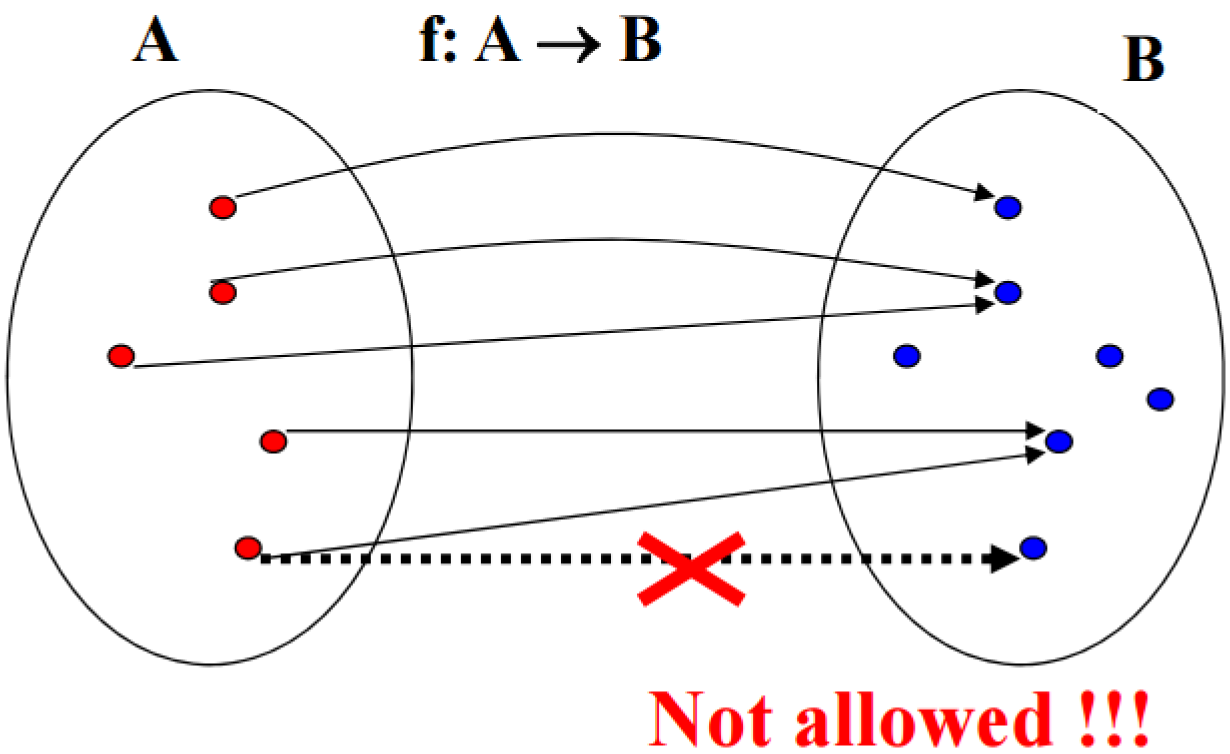
Union: $A \vee B = 11001$ – $\{1, 2, 5\}$
Intersection: $A \wedge B = 00001 = \{5\}$
Complement: $\bar{A} = 10110 = \{1, 3, 4\}$

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.



- 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.



Representing Functions

- Explicitly state the assignments between elements of the two sets
- By a formula

Representing Functions

- Explicitly state the assignments between elements of the two sets
- By a formula

Example 1:

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

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

Representing Functions

- Explicitly state the assignments between elements of the two sets
- By a formula

Example 2:

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

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

Representing Functions

- Explicitly state the assignments between elements of the two sets
- By a formula

Example 3:

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

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

Important Sets of Functions

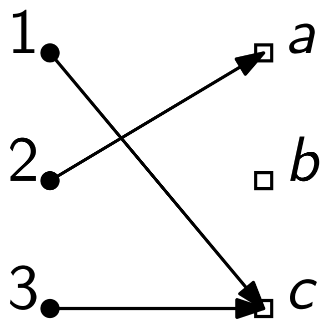
- Let f be a function from A to B. We say that A is the *domain* of f and B is the *codomain* of f. If $f(a) = b$, b is called *the image* of a and a is a *preimage* of b. The *range of f* is the set of all images of elements of A, denoted by $f(A)$. We also say *f maps A to B*.

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:

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



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:

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

– c is the image of 1
– 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 $\{a, c\}$

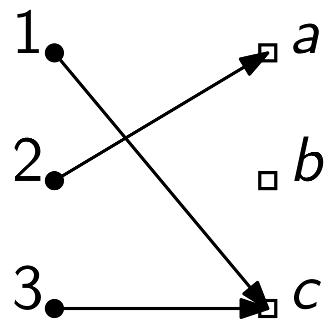


Image of a Subset

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

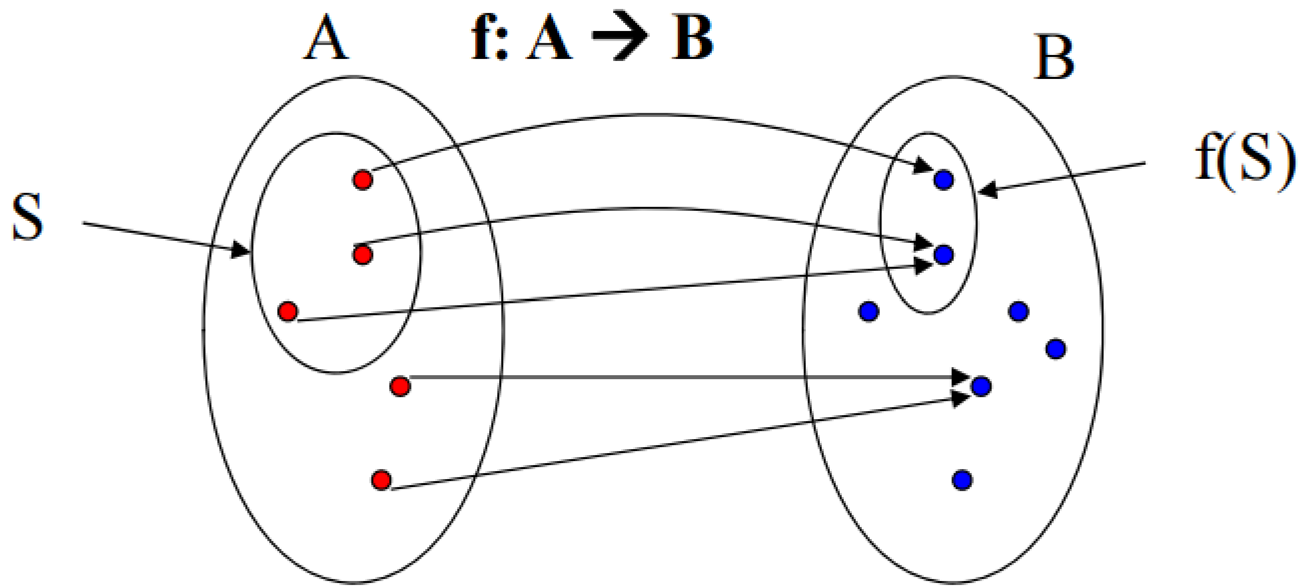
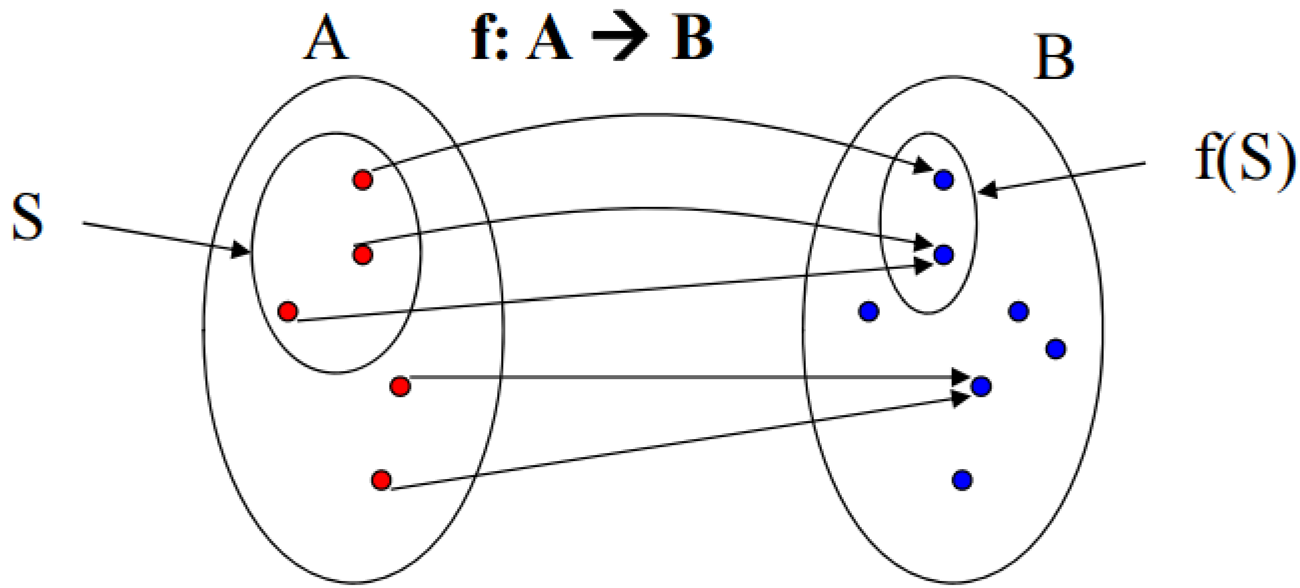
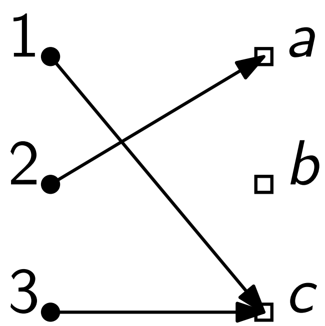


Image of a Subset

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





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

Injective (One-to-One) 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. In this case, f is called an *injection*.

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

Injective (One-to-One) Function

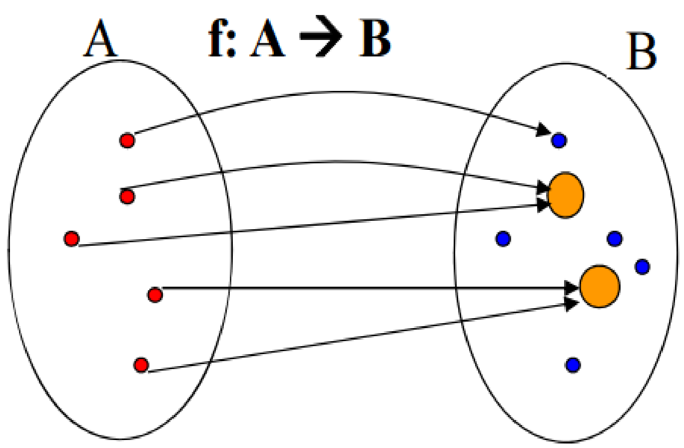
- A function f is called *one-to-one* or *injective*, if and only if $f(x) = f(y)$ implies $x = y$ for all x, y in the domain of f. In this case, f is called an *injection*.

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

Injective (One-to-One) 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. In this case, f is called an *injection*.

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

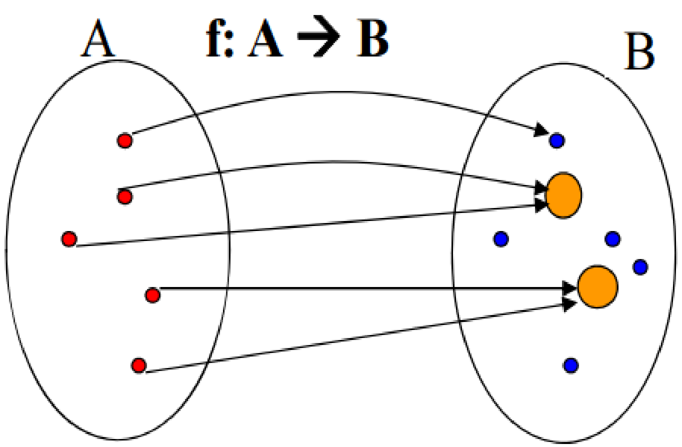


Not injective

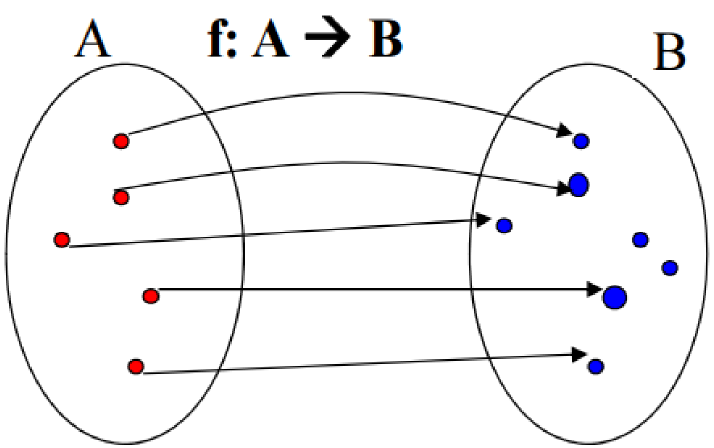
Injective (One-to-One) Function

- 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. In this case, f is called an *injection*.

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



Not injective



Injective function

Injective Functions

- **Example 1**:

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

  Define f as

  – $1 \mapsto c$

  – $2 \mapsto a$

  – $3 \mapsto c$

  Is f one-to-one?

Injective Functions

- **Example 1**:

  $A = \{1, 2, 3\}$, $B = \{a, b, c\}$
  Define f as
  - $1 \mapsto c$
  - $2 \mapsto a$
  - $3 \mapsto c$

  Is f one-to-one?

- **Example 2**:

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

  Is g one-to-one?

Surjective (Onto) 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 $f(a) = b$. In this case, f is called a *surjection*.

Surjective (Onto) Function

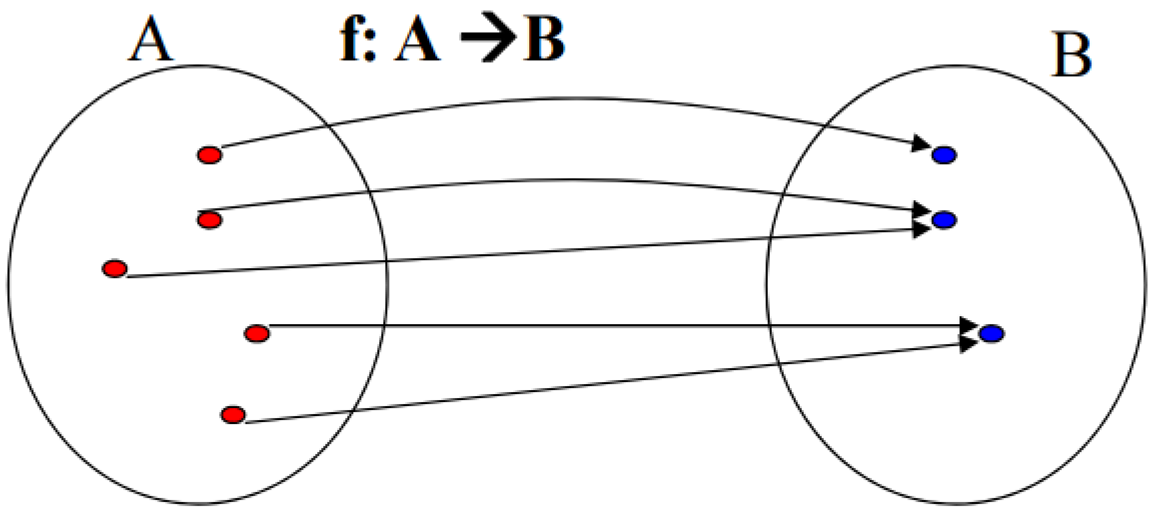
- A function f is called *onto* or *surjective*, if and only if for every $b \in B$ there is an element $a \in A$ such that $f(a) = b$. In this case, f is called a *surjection*.

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

Surjective (Onto) 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 $f(a) = b$. In this case, f is called a *surjection*.

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



Surjective Functions

- **Example 1**:

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

  Define f as

  – $1 \mapsto c$

  – $2 \mapsto a$

  – $3 \mapsto c$

  Is f onto?

Surjective Functions

- **Example 1**:

  $A = \{1, 2, 3\}$, $B = \{a, b, c\}$
  Define f as
  - $1 \mapsto c$
  - $2 \mapsto a$
  - $3 \mapsto c$

  Is f onto?

- **Example 2**:

  Let $A = \{0, 1, \ldots, 9\}$, $B = \{0, 1, 2\}$
  Define $h : A \to B$ as $h(x) = x \bmod 3$.

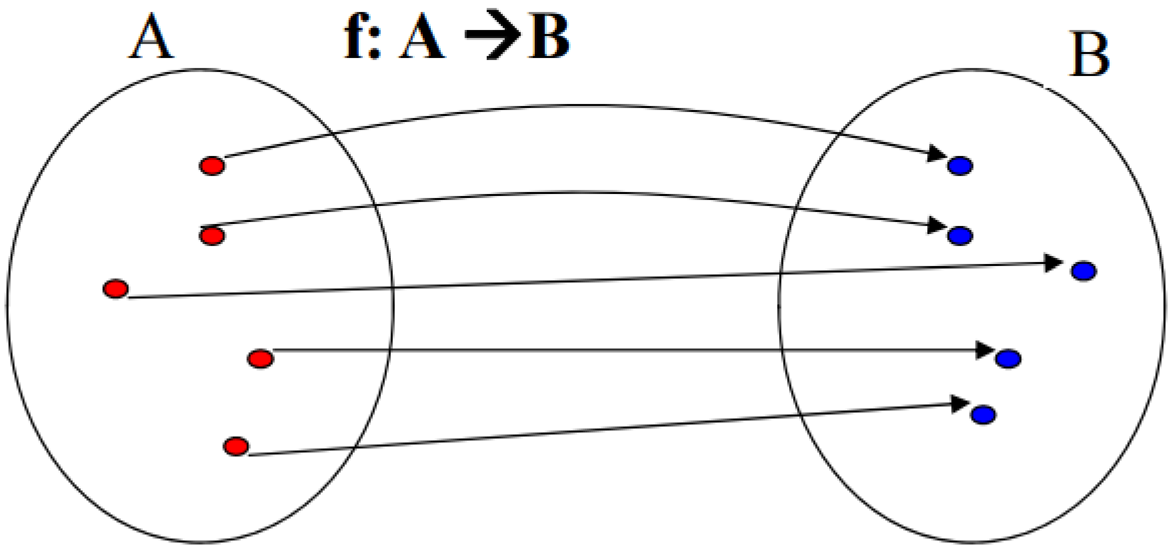
  Is h onto?

Bijective Function (One-to-One Correspondence)

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

Bijective Function (One-to-One Correspondence)

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



Bijective Functions

- **Example 1**:

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

  Define f as

  – $1 \mapsto c$

  – $2 \mapsto a$

  – $3 \mapsto b$

  Is f bijective?

Bijective Functions

- **Example 1**:

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

  Define f as

  – $1 \mapsto c$

  – $2 \mapsto a$

  – $3 \mapsto b$

  Is f bijective?

- **Example 2**:

  Define $g : \mathbf{N} \to \mathbf{N}$ as $g(x) = \lfloor \frac{x}{2} \rfloor$ (floor function).

  Is g bijective?

Summary

- Suppose that $f : A \to B$.

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

Note

- 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."

Note

- 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."

Proof.

$\diamond$ only if part: Suppose that f is one-to-one. Let $\{x_1, x_2, \ldots, x_n\}$ be elements of A. Then $f(x_i) \neq f(x_j)$ for $i \neq j$. Therefore, $|f(A)| = |\{f(x_1), \ldots, f(x_n)\}| = n$. But $|B| = n$ and $f(A) \subseteq B$. Therefore, $f(A) = B$.

$\diamond$ if part: Suppose that f is onto. Let $A = \{x_1, x_2, \ldots, x_n\}$ be a listing of the elements of A. Suppose that $f(x_i) = f(x_j)$ for some $i \neq j$. Then, $|\{f(x_1), \ldots, f(x_n)\}| \leq n - 1$. But $|f(A)| = |B| = n$, a contradiction.

Bijective Function

- "For a function f from A to itself, f is one-to-one if and only if f is onto, where A is infinite." Is this true?

Bijective Function

- "For a function f from A to itself, f is one-to-one if and only if f is onto, where A is infinite." Is this true?

Counterexample:

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

f is one-to-one but not onto

- $1 \mapsto 2$
- $2 \mapsto 4$
- $3 \mapsto 6$

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 form A to $\mathbf{R}$ defined for all $x \in A$ by

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

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 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:

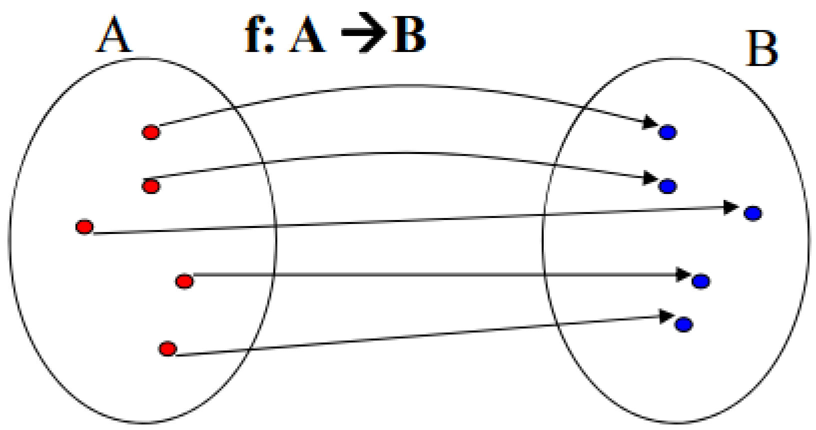
$f_1 = x - 1$ and $f_2 = x^3 + 1$

Then

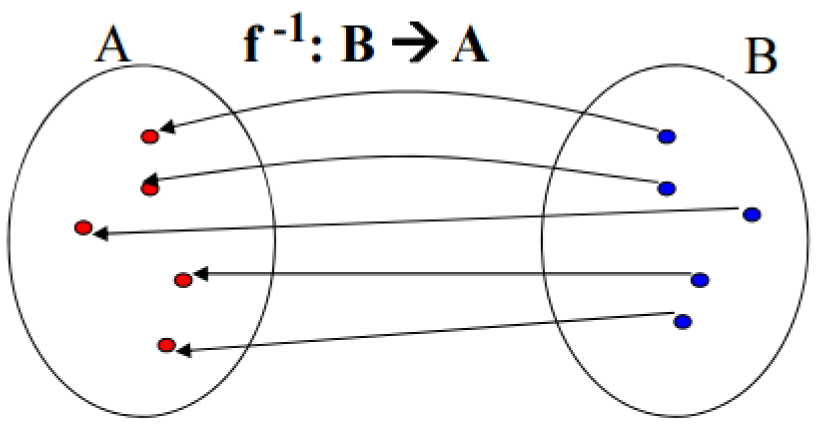
$$(f_1 + f_2)(x) = x^3 + x$$
$$(f_1 f_2)(x) = x^4 - x^3 + x - 1$$

Inverse Functions

- Let $f : A \to B$ be a bijection. The *inverse of f* is the function that assigns to an element b belonging to B the unique element a in A such that $f(a) = b$, 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

- Note: if f is not a bijection, it is impossible to define the inverse function of f. Why ?

Inverse Functions

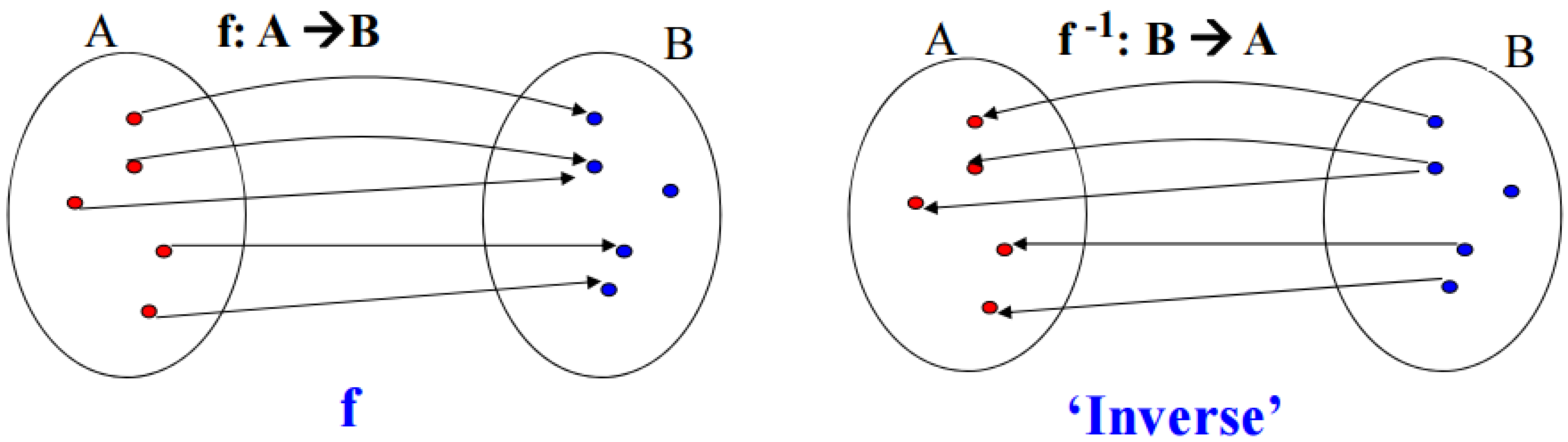
- Note: if f is not a bijection, it is impossible to define the inverse function of f. Why ?

Assume f is not injective:

Inverse Functions

- Note: if f is not a bijection, it is impossible to define the inverse function of f. Why ?

Assume f is not injective:



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

Inverse Functions

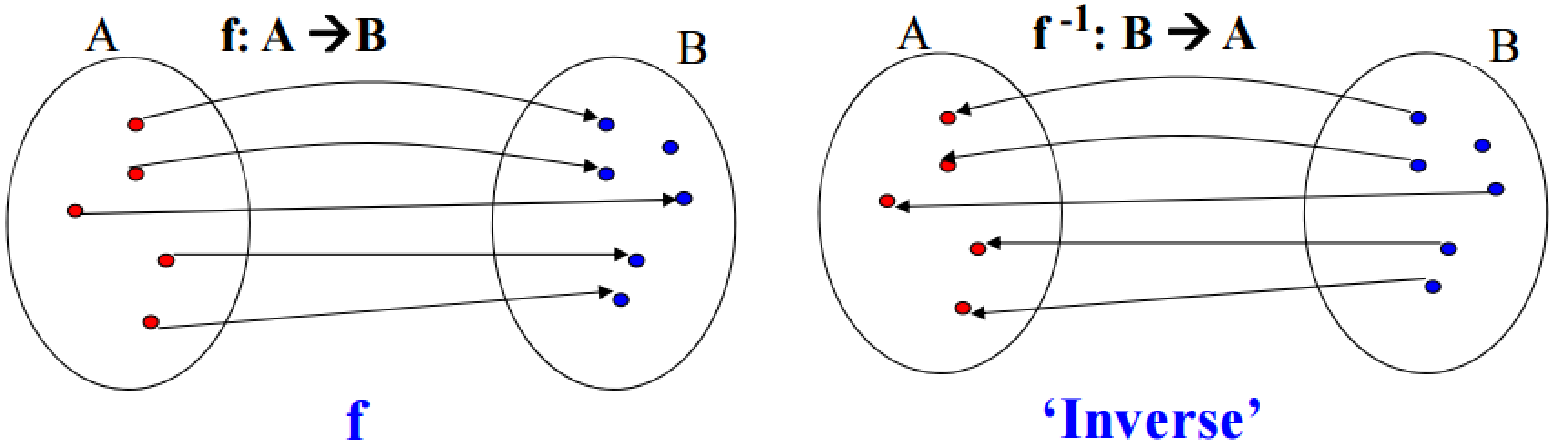
- Note: if f is not a bijection, it is impossible to define the inverse function of f. Why ?

  Assume f is not surjective:

Inverse Functions

- Note: if f is not a bijection, it is impossible to define the inverse function of f. Why ?

Assume f is not surjective:



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

- **Example 1**:

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

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

Inverse Functions

- **Example 1**:

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

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

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

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?

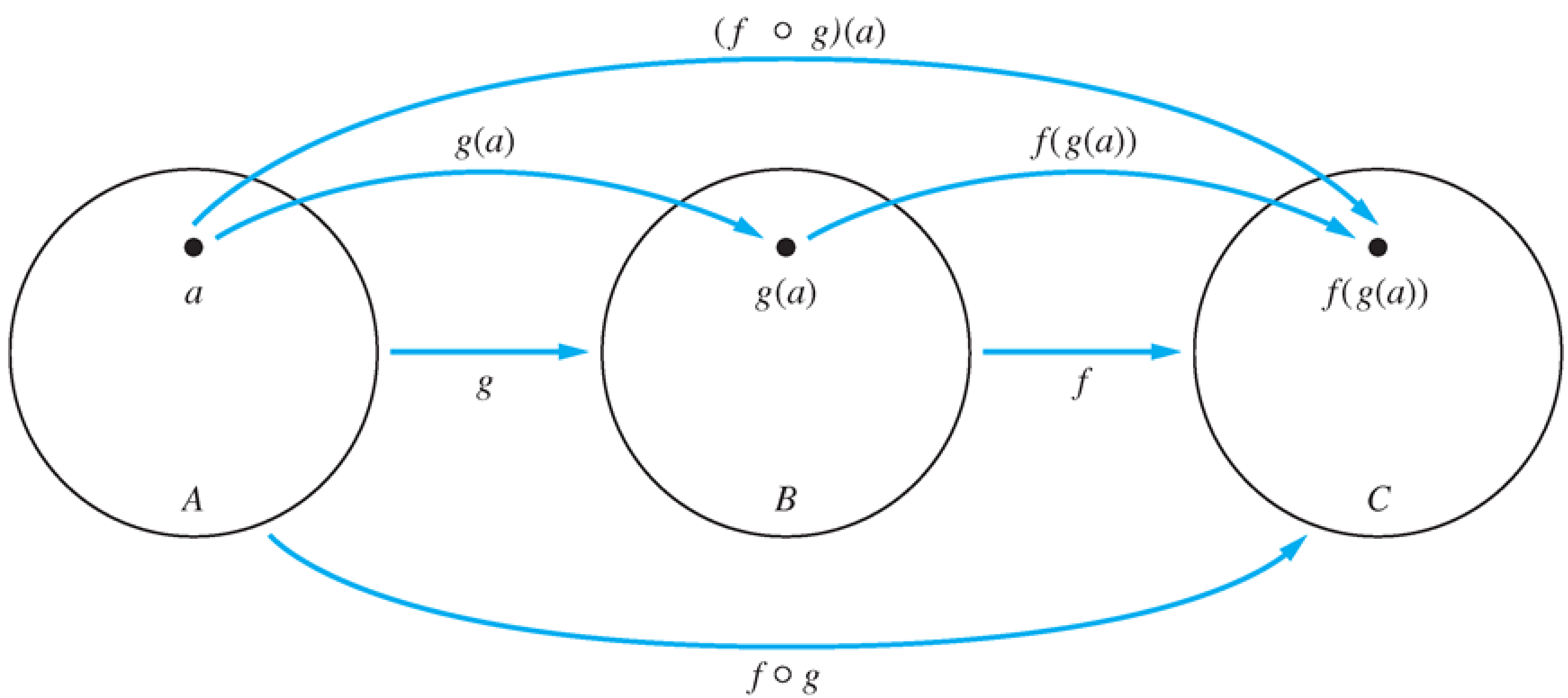
  No, since f is not onto.

Composition of Functions

- Let f be a function from B to C and let g be a function from 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

- Let f be a function from B to C and let g be a function from 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**:

  Let $A = \{1, 2, 3\}$ and $B = \{a, b, c, d\}$.

  $g : A \to A$ $f : A \to B$

  $1 \mapsto 3$ $1 \mapsto b$

  $2 \mapsto 1$ $2 \mapsto a$

  $3 \mapsto 2$ $3 \mapsto d$

  What is $f \circ g$?

Composition of Functions

- **Example 1**:

  Let $A = \{1, 2, 3\}$ and $B = \{a, b, c, d\}$.

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

  What is $f \circ g$?

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

- **Example 2**:

  Let $f : \mathbf{Z} \rightarrow \mathbf{Z}$ and $g : \mathbf{Z} \rightarrow \mathbf{Z}$, where $f(x) = 2x$ and $g(x) = x^2$.

  What are $g \circ f$ and $f \circ g$?

Composition of Functions

- **Example 2**:

  Let $f : \mathbf{Z} \to \mathbf{Z}$ and $g : \mathbf{Z} \to \mathbf{Z}$, where $f(x) = 2x$ and $g(x) = x^2$.

  What are $g \circ f$ and $f \circ g$?

  $g \circ f : \mathbf{Z} \to \mathbf{Z}$ $\quad g \circ f = 4x^2$

  $f \circ g : \mathbf{Z} \to \mathbf{Z}$ $\quad f \circ g = 2x^2$

Composition of Functions

- **Example 2**:

  Let $f : \mathbf{Z} \to \mathbf{Z}$ and $g : \mathbf{Z} \to \mathbf{Z}$, where $f(x) = 2x$ and $g(x) = x^2$.

  What are $g \circ f$ and $f \circ g$?

  $g \circ f : \mathbf{Z} \to \mathbf{Z}$ $\quad g \circ f = 4x^2$

  $f \circ g : \mathbf{Z} \to \mathbf{Z}$ $\quad f \circ g = 2x^2$

  Note: In general, the order of composition matters.

Composition of Functions

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

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 *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 $\lceil x \rceil$.

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

Some Important Functions

Ex. 1: Prove or disprove that if x is a real number, then $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

Ex. 2: Prove or disprove that $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$ for all real numbers x and y.

Some Important Functions

Ex. 1: Prove or disprove that if x is a real number, then $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

Ex. 2: Prove or disprove that $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$ for all real numbers x and y.

- The factorial function $f : \mathbf{N} \to \mathbf{Z}^+$ is the product of the first n positive integers when n is a nonnegative integer, denoted by $f(n) = n!$.

Next Lecture

- functions, complexity ...