Lecture 6: Functions

Xiaoxing Ma

Nanjing University

xxm@nju.edu.cn

November 6, 2017

Acknowledgement: These Beamer slides are totally based on the textbook *Discrete Mathematical Structures*, by B. Kolman, R. C. Busby and S. C. Ross, and Prof. Daoxu Chen's PowerPoint slides.

At the Last Class

1. Basic Operations on Relations
   - Set operations on relations
   - Inverse
   - Composition
   - Closure of Relation
2. Computer Representation and Warshall's Algorithm
   - item Representation of Relations in Computer
   - Transitive closure and Warshall's Algorithm

Overview

1. Basics of Functions
   - Function as a class of special relations
   - Types of functions
   - Function and comparison of set size

2. Functions and Computer Science
   - Commonly used functions in computer applications
   - Growth of functions
   - Permutation: bijection on one set

Definition of Function

Definition

Let A and B be nonempty sets. A **function** f from A to B, which is denoted by $f : A \to B$, is a relation from A to B such that for all $a \in A$, $f(a)$ contains just one element of B.

- A special kind of binary relation
- Under f, each element in the domain of f has a unique value.
- If A, B are nonempty finite sets, there are $|B|^{|A|}$ different functions from A to B.

Image and Counterimage

Definition

Let $f : A \to B$, $A' \subseteq A$, then $f(A') = \{y | y = f(x), x \in A'\}$ is called the **image** of A' under f.

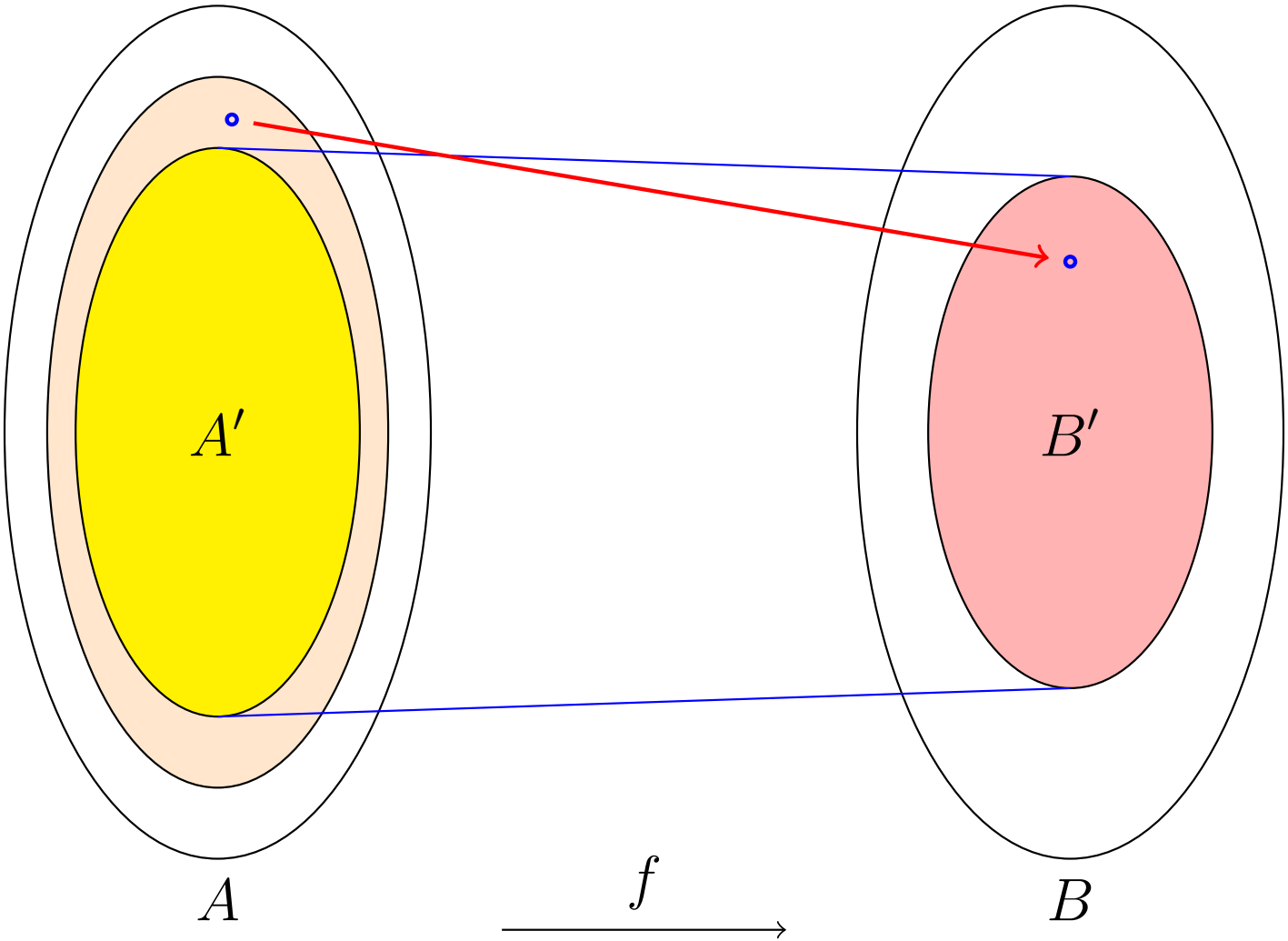
- An element in $Dom(f)$ corresponds a value
- A subset of $Dom(f)$ corresponds an image

Definition

Let $B' \subseteq B$, then $f^{-1}(B') = \{x | x \in A, f(x) \in B'\}$ is called the **counterimage** of B' under f.

Note: $A' \subseteq f^{-1}(f(A'))$ for all $A' \subseteq A$, but the equality is not necessarily holding.

Image and Counterimage



Special Types of Functions

Surjection: $f : A \to B$ is a surjection or "onto" $\iff$ $Ran(f) = B, \iff \forall y \in B, \exists x \in A$, such that $f(x) = y$

Injection: $f : A \to B$ is a injection or "one-to-one" $\iff \forall y \in Ran(f)$, there is at most one $x \in A$, such that $f(x) = y$ $\iff \forall x_1, x_2 \in A$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$ $\iff \forall x_1, x_2 \in A$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$

Bijection: (one-to-one correspondence), surjection plus injection.

Special Types of Functions

Surjection: $f : A \to B$ is a surjection or "onto" $\iff$ $Ran(f) = B$, $\iff$ $\forall y \in B, \exists x \in A$, such that $f(x) = y$

Injection: $f : A \to B$ is a injection or "one-to-one"
$\iff$ $\forall y \in Ran(f)$, there is at most one $x \in A$, such that $f(x) = y$
$\iff$ $\forall x_1, x_2 \in A$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$
$\iff$ $\forall x_1, x_2 \in A$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$

Bijection: (one-to-one correspondence), surjection plus injection.

Special Types of Functions

Surjection: $f : A \to B$ is a surjection or "onto" $\iff$ $Ran(f) = B$, $\iff$ $\forall y \in B, \exists x \in A$, such that $f(x) = y$

Injection: $f : A \to B$ is a injection or "one-to-one"

$\iff$ $\forall y \in Ran(f)$, there is at most one $x \in A$, such that $f(x) = y$

$\iff$ $\forall x_1, x_2 \in A$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$

$\iff$ $\forall x_1, x_2 \in A$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$

Bijection: (one-to-one correspondence), surjection plus injection.

Special Types of Functions

Surjection: $f : A \to B$ is a surjection or "onto" $\iff$ $Ran(f) = B$, $\iff$ $\forall y \in B, \exists x \in A$, such that $f(x) = y$

Injection:

$f : A \to B$ is a injection or "one-to-one"

$\iff$ $\forall y \in Ran(f)$, there is at most one $x \in A$, such that $f(x) = y$

$\iff$ $\forall x_1, x_2 \in A$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$

$\iff$ $\forall x_1, x_2 \in A$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$

Bijection: (one-to-one correspondence), surjection plus injection.

Special Types of Functions

Surjection: $f : A \to B$ is a surjection or "onto" $\iff$ $Ran(f) = B$, $\iff$ $\forall y \in B, \exists x \in A$, such that $f(x) = y$

Injection:

$f : A \to B$ is a injection or "one-to-one"

$\iff$ $\forall y \in Ran(f)$, there is at most one $x \in A$, such that $f(x) = y$

$\iff$ $\forall x_1, x_2 \in A$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$

$\iff$ $\forall x_1, x_2 \in A$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$

Bijection: (one-to-one correspondence), surjection plus injection.

Special Types of Functions

Surjection: $f : A \to B$ is a surjection or "onto" $\iff$ $Ran(f) = B$, $\iff$ $\forall y \in B, \exists x \in A$, such that $f(x) = y$

Injection:

$f : A \to B$ is a injection or "one-to-one"

$\iff$ $\forall y \in Ran(f)$, there is at most one $x \in A$, such that $f(x) = y$

$\iff$ $\forall x_1, x_2 \in A$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$

$\iff$ $\forall x_1, x_2 \in A$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$

Bijection: (one-to-one correspondence), surjection plus injection.

Special Types of Functions

Surjection: $f : A \to B$ is a surjection or "onto" $\iff$ $Ran(f) = B$, $\iff$ $\forall y \in B, \exists x \in A$, such that $f(x) = y$

Injection:

$f : A \to B$ is a injection or "one-to-one"

$\iff$ $\forall y \in Ran(f)$, there is at most one $x \in A$, such that $f(x) = y$

$\iff$ $\forall x_1, x_2 \in A$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$

$\iff$ $\forall x_1, x_2 \in A$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$

Bijection: (one-to-one correspondence), surjection plus injection.

Special Types of Functions

Example

- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = -x^2 + 2x - 1$
- $f : \mathbb{Z}^+ \to \mathbb{R}$, $f(x) = \ln x$, one-to-one
- $f : \mathbb{R} \to \mathbb{Z}$, $f(x) = \lfloor x \rfloor$, onto
- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x - 1$, bijection
- $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x) = \dfrac{x^2 + 1}{x}$
- $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $f(\langle x, y \rangle) = \langle x + y, x - y \rangle$, bijection
  Note: $f(\{\langle x, y \rangle | x, y \in \mathbb{R}, y = x + 1\}) = \mathbb{R} \times \{-1\}$
- $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(\langle x, y \rangle) = |x^2 - y^2|$
  Note: $f(\mathbb{N} \times 0) = \{n^2 | n \in \mathbb{N}\}$, but $f^{-1}(\{0\}) = \{\langle n, n \rangle | n \in \mathbb{N}\}$

Special Types of Functions

Example

- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = -x^2 + 2x - 1$
- $f : \mathbb{Z}^+ \to \mathbb{R}$, $f(x) = \ln x$, one-to-one
- $f : \mathbb{R} \to \mathbb{Z}$, $f(x) = \lfloor x \rfloor$, onto
- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x - 1$, bijection
- $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x) = \dfrac{x^2 + 1}{x}$
- $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $f(\langle x, y \rangle) = \langle x + y, x - y \rangle$, bijection
  Note: $f(\{\langle x, y \rangle | x, y \in \mathbb{R}, y = x + 1\}) = \mathbb{R} \times \{-1\}$
- $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(\langle x, y \rangle) = |x^2 - y^2|$
  Note: $f(\mathbb{N} \times 0) = \{n^2 | n \in \mathbb{N}\}$, but $f^{-1}(\{0\}) = \{\langle n, n \rangle | n \in \mathbb{N}\}$

Special Types of Functions

Example

- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = -x^2 + 2x - 1$
- $f : \mathbb{Z}^+ \to \mathbb{R}$, $f(x) = \ln x$, one-to-one
- $f : \mathbb{R} \to \mathbb{Z}$, $f(x) = \lfloor x \rfloor$, onto
- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x - 1$, bijection
- $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x) = \dfrac{x^2 + 1}{x}$
- $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $f(\langle x, y \rangle) = \langle x + y, x - y \rangle$, bijection
  Note: $f(\{\langle x, y \rangle | x, y \in \mathbb{R}, y = x + 1\}) = \mathbb{R} \times \{-1\}$
- $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(\langle x, y \rangle) = |x^2 - y^2|$
  Note: $f(\mathbb{N} \times 0) = \{n^2 | n \in \mathbb{N}\}$, but $f^{-1}(\{0\}) = \{\langle n, n \rangle | n \in \mathbb{N}\}$

Special Types of Functions

Example

- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = -x^2 + 2x - 1$
- $f : \mathbb{Z}^+ \to \mathbb{R}$, $f(x) = \ln x$, one-to-one
- $f : \mathbb{R} \to \mathbb{Z}$, $f(x) = \lfloor x \rfloor$, onto
- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x - 1$, bijection
- $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x) = \dfrac{x^2 + 1}{x}$
- $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $f(\langle x, y \rangle) = \langle x + y, x - y \rangle$, bijection
  Note: $f(\{\langle x, y \rangle | x, y \in \mathbb{R}, y = x + 1\}) = \mathbb{R} \times \{-1\}$
- $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(\langle x, y \rangle) = |x^2 - y^2|$
  Note: $f(\mathbb{N} \times 0) = \{n^2 | n \in \mathbb{N}\}$, but $f^{-1}(\{0\}) = \{\langle n, n \rangle | n \in \mathbb{N}\}$

Special Types of Functions

Example

- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = -x^2 + 2x - 1$
- $f : \mathbb{Z}^+ \to \mathbb{R}$, $f(x) = \ln x$, one-to-one
- $f : \mathbb{R} \to \mathbb{Z}$, $f(x) = \lfloor x \rfloor$, onto
- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x - 1$, bijection
- $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x) = \dfrac{x^2 + 1}{x}$
- $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $f(\langle x, y \rangle) = \langle x + y, x - y \rangle$, bijection
  Note: $f(\{\langle x, y \rangle | x, y \in \mathbb{R}, y = x + 1\}) = \mathbb{R} \times \{-1\}$
- $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(\langle x, y \rangle) = |x^2 - y^2|$
  Note: $f(\mathbb{N} \times 0) = \{n^2 | n \in \mathbb{N}\}$, but $f^{-1}(\{0\}) = \{\langle n, n \rangle | n \in \mathbb{N}\}$

Special Types of Functions

Example

- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = -x^2 + 2x - 1$
- $f : \mathbb{Z}^+ \to \mathbb{R}$, $f(x) = \ln x$, one-to-one
- $f : \mathbb{R} \to \mathbb{Z}$, $f(x) = \lfloor x \rfloor$, onto
- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x - 1$, bijection
- $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x) = \dfrac{x^2 + 1}{x}$
- $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $f(\langle x, y \rangle) = \langle x + y, x - y \rangle$, bijection
  Note: $f(\{\langle x, y \rangle | x, y \in \mathbb{R}, y = x + 1\}) = \mathbb{R} \times \{-1\}$
- $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(\langle x, y \rangle) = |x^2 - y^2|$
  Note: $f(\mathbb{N} \times 0) = \{n^2 | n \in \mathbb{N}\}$, but $f^{-1}(\{0\}) = \{\langle n, n \rangle | n \in \mathbb{N}\}$

Special Types of Functions

Example

- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = -x^2 + 2x - 1$
- $f : \mathbb{Z}^+ \to \mathbb{R}$, $f(x) = \ln x$, one-to-one
- $f : \mathbb{R} \to \mathbb{Z}$, $f(x) = \lfloor x \rfloor$, onto
- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x - 1$, bijection
- $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x) = \dfrac{x^2 + 1}{x}$
- $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $f(\langle x, y \rangle) = \langle x + y, x - y \rangle$, bijection
  Note: $f(\{\langle x, y \rangle | x, y \in \mathbb{R}, y = x + 1\}) = \mathbb{R} \times \{-1\}$
- $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(\langle x, y \rangle) = |x^2 - y^2|$
  Note: $f(\mathbb{N} \times 0) = \{n^2 | n \in \mathbb{N}\}$, but $f^{-1}(\{0\}) = \{\langle n, n \rangle | n \in \mathbb{N}\}$

Characteristic Function of Set

Definition

Let U is the universal set, for any $A \subseteq U$, the **characteristic function** of A, $\chi_A : U \to \{0, 1\}$ is defined as $\chi_A(x) = 1$ *iff.* $x \in A$.

Note the one-to-one correspondence between $\mathcal{P}(U)$, the power set of U, and the set of all possible characteristic functions of A, $\chi_A : U \to \{0, 1\}$.

Natural Function

Definition

R is an equivalence relation on set A, $g : A \to A/R$, for all $a \in A$, $g(a) = R(a)$, then g is called a **natural function** on A.

Natural function is surjection: For any $R(a) \in A/R$, there exists some $x \in A$, such that $g(x) = R(x)$.

Images of Union and Intersection

Given $f : A \to B$, and X, Y are subsets of A, then:

- $f(X \cup Y) = f(X) \cup f(Y)$
- $f(X \cap Y) \subseteq f(X) \cap f(Y)$

Example (Counterexample for $f(X \cap Y) = f(X) \cap f(Y)$)

$a \in X$, but $a \notin Y$, and $b \in Y$, but $b \notin X$. $f(a) = f(b) = c$. then, $c \in f(X) \cap f(Y)$, but, maybe $c \notin f(X \cap Y)$.

Images of Union and Intersection

Given $f : A \to B$, and X, Y are subsets of A, then:

- $f(X \cup Y) = f(X) \cup f(Y)$
- $f(X \cap Y) \subseteq f(X) \cap f(Y)$

Example (Counterexample for $f(X \cap Y) = f(X) \cap f(Y)$)

$a \in X$, but $a \notin Y$, and $b \in Y$, but $b \notin X$. $f(a) = f(b) = c$. then, $c \in f(X) \cap f(Y)$, but, maybe $c \notin f(X \cap Y)$.

Composition of Functions

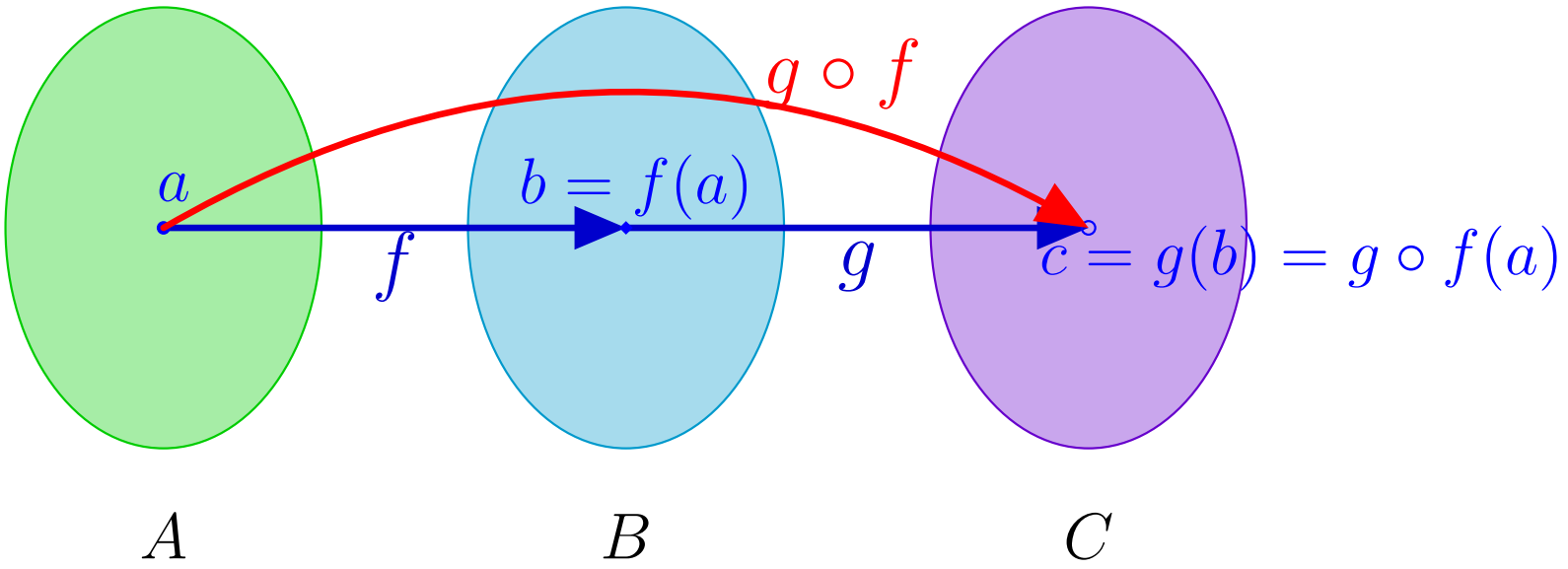
Since function is relation as well, the composition of relation can be applied for functions, with the results being relation.

The composition of functions is still function.

Proof.

Suppose $f : A \to B$, $g : B \to C$, $g \circ f$ is a relation from A to C. $\forall x \in A$, we have $g \circ f(x) = g(f(x))$. It is easy to prove that for every a in A, there is just one c in C, such that $g(f(a)) = c$. So, $g \circ f$ is a function. $\square$

Composition of Functions



Associative Law

The composition of functions is simply the composition of relations, so it is an associative operation.

For any functions $f : A \to B$, $g : B \to C$, $h : C \to D$,

$$(h \circ g) \circ f = h \circ (g \circ f)$$

Composition of Surjections

If $f : A \to B$, $g : B \to C$ are both surjections, then $g \circ f : A \to C$ is also surjection.

Proof.

Sketch of proof: For any $y \in C$, since g is a surjection, there must be some $t \in B$, such that $g(t) = y$. Similarily, since f is surjection, there must be some $x \in A$, such that $f(x) = t$, so, $g \circ f(x) = y$. □

However, if $g \circ f$ is a surjection, can it be derived that f and g are both surjections as well?

Obviously, g must be a surjection.
If there is some $t \in B$, for any $x \in A$, $f(x) \neq t$, (i.e. f is not a surjection!) then if only $g(B - \{t\}) = C$, $g \circ f$ is still a surjection.

Composition of Surjections

If $f : A \to B$, $g : B \to C$ are both surjections, then $g \circ f : A \to C$ is also surjection.

Proof.

Sketch of proof: For any $y \in C$, since g is a surjection, there must be some $t \in B$, such that $g(t) = y$. Similarily, since f is surjection, there must be some $x \in A$, such that $f(x) = t$, so, $g \circ f(x) = y$. □

However, if $g \circ f$ is a surjection, can it be derived that f and g are both surjections as well?

Obviously, g must be a surjection.
If there is some $t \in B$, for any $x \in A$, $f(x) \neq t$, (i.e. f is not a surjection!) then if only $g(B - \{t\}) = C$, $g \circ f$ is still a surjection.

Composition of Surjections

If $f : A \to B$, $g : B \to C$ are both surjections, then $g \circ f : A \to C$ is also surjection.

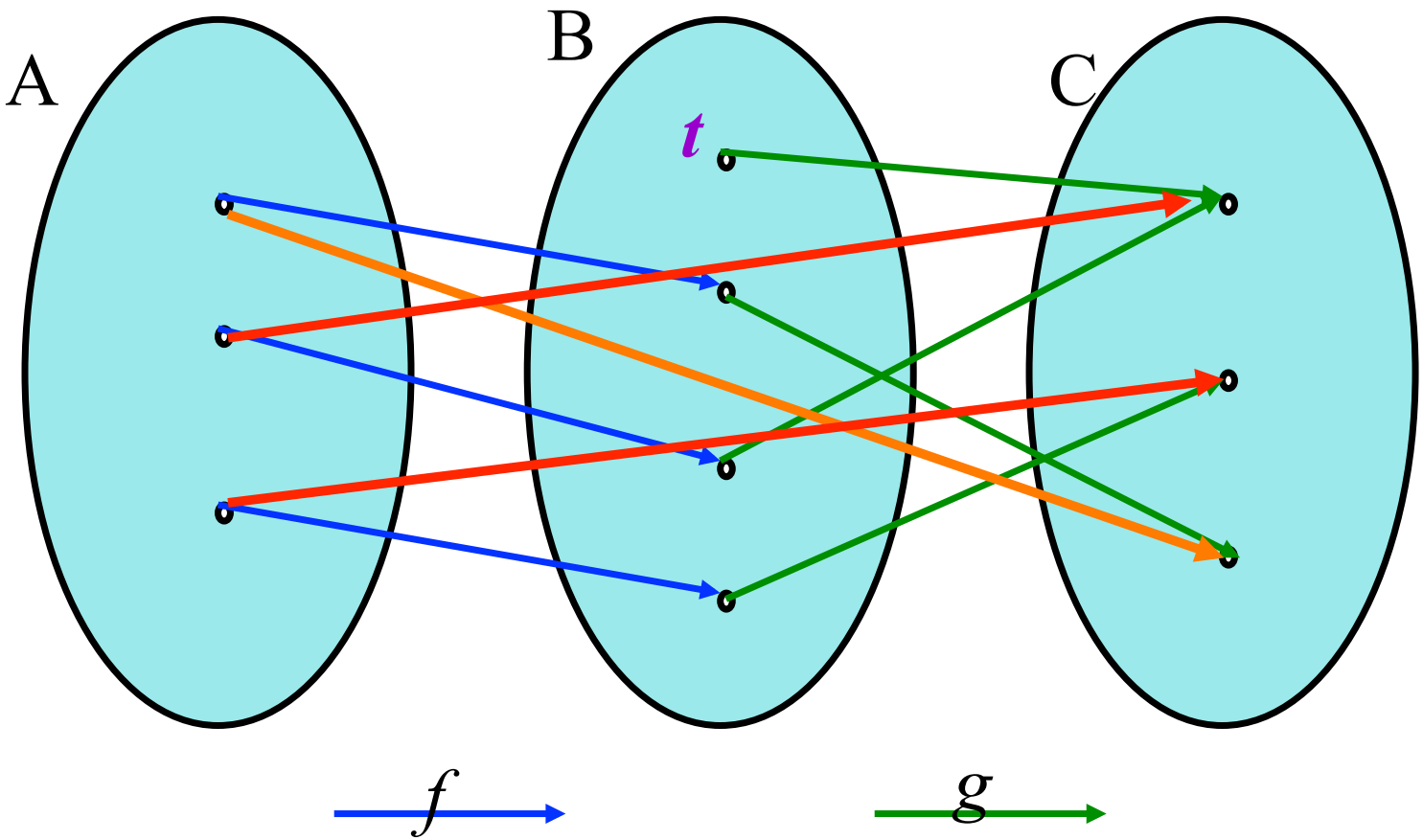
Proof.

Sketch of proof: For any $y \in C$, since g is a surjection, there must be some $t \in B$, such that $g(t) = y$. Similarily, since f is surjection, there must be some $x \in A$, such that $f(x) = t$, so, $g \circ f(x) = y$. □

However, if $g \circ f$ is a surjection, can it be derived that f and g are both surjections as well?

Obviously, g must be a surjection.
If there is some $t \in B$, for any $x \in A$, $f(x) \neq t$, (i.e. f is not a surjection!) then if only $g(B - \{t\}) = C$, $g \circ f$ is still a surjection.

Composition is a Surjection



Composition of Injections

If $f : A \to B$, $g : B \to C$ are both injections, then $g \circ f : A \to C$ is a injection as well.

Proof.

Sketch of proof: By contradiction, suppose $x_1, x_2 \in A$, and $x_1 \neq x_2$, but $g \circ f(x_1) = g \circ f(x_2)$, let $f(x_1) = t_1$, $f(x_2) = t_2$, if $t_1 = t_2$, then f is not a injection, if $t_1 \neq t_2$, then g is not a injection. □

If $g \circ f$ is a injection, can it be derived that f and g are both injections?

Obviously, f must be a injection.
Suppose that $t_1, t_2 \in B$, $t_1 \neq t_2$, but $g(t_1) = g(t_2)$, (i.e. g is not a injection!) If only t_1 or t_2 are not in $Ran(f)$, then $g \circ f$ still may be injection.

Composition of Injections

If $f : A \to B$, $g : B \to C$ are both injections, then $g \circ f : A \to C$ is a injection as well.

Proof.

Sketch of proof: By contradiction, suppose $x_1, x_2 \in A$, and $x_1 \neq x_2$, but $g \circ f(x_1) = g \circ f(x_2)$, let $f(x_1) = t_1$, $f(x_2) = t_2$, if $t_1 = t_2$, then f is not a injection, if $t_1 \neq t_2$, then g is not a injection. □

If $g \circ f$ is a injection, can it be derived that f and g are both injections?

Obviously, f must be a injection.
Suppose that $t_1, t_2 \in B$, $t_1 \neq t_2$, but $g(t_1) = g(t_2)$, (i.e. g is not a injection!) If only t_1 or t_2 are not in $Ran(f)$, then $g \circ f$ still may be injection.

Composition of Injections

If $f : A \to B$, $g : B \to C$ are both injections, then $g \circ f : A \to C$ is a injection as well.

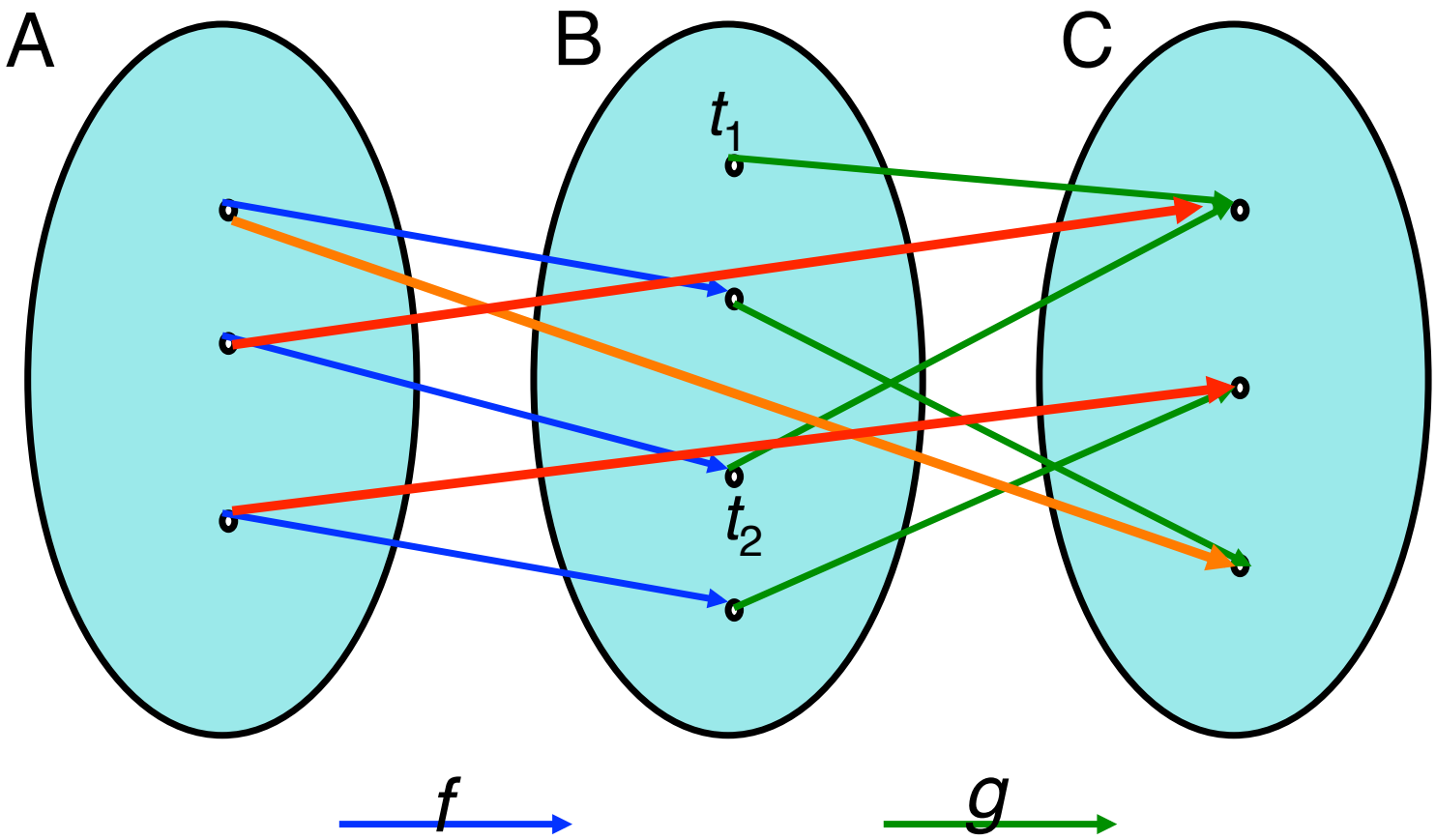
Proof.

Sketch of proof: By contradiction, suppose $x_1, x_2 \in A$, and $x_1 \neq x_2$, but $g \circ f(x_1) = g \circ f(x_2)$, let $f(x_1) = t_1$, $f(x_2) = t_2$, if $t_1 = t_2$, then f is not a injection, if $t_1 \neq t_2$, then g is not a injection. □

If $g \circ f$ is a injection, can it be derived that f and g are both injections?

Obviously, f must be a injection.
Suppose that $t_1, t_2 \in B$, $t_1 \neq t_2$, but $g(t_1) = g(t_2)$, (i.e. g is not a injection!) If only t_1 or t_2 are not in $Ran(f)$, then $g \circ f$ still may be injection.

Composition is a Injection



Identity Function on a Set

Definition

1_A is the **identity function** on A: $1_A(x) = x$ for all $x \in A$.

Theorem

For any $f : A \to B$, $f = 1_B \circ f = f \circ 1_A$

Proof.

Sketch of proof: Proving that the set f is equal to the set $f \circ 1_A$ and $1_B \circ f$. □

Note: if $\langle x, y \rangle \in f$, then $\langle x, y \rangle \in f$ and $\langle x, x \rangle \in 1_A$;
if $\langle x, y \rangle \in f \circ 1_A$, then there must be a $\langle t, y \rangle \in f$, and $\langle x, t \rangle \in 1_A$, then $t = x$, so $\langle x, y \rangle \in f$.

Identity Function on a Set

Definition

1_A is the **identity function** on A: $1_A(x) = x$ for all $x \in A$.

Theorem

For any $f : A \to B$, $f = 1_B \circ f = f \circ 1_A$

Proof.

Sketch of proof: Proving that the set f is equal to the set $f \circ 1_A$ and $1_B \circ f$. □

Note: if $\langle x, y \rangle \in f$, then $\langle x, y \rangle \in f$ and $\langle x, x \rangle \in 1_A$;
if $\langle x, y \rangle \in f \circ 1_A$, then there must be a $\langle t, y \rangle \in f$, and $\langle x, t \rangle \in 1_A$, then $t = x$, so $\langle x, y \rangle \in f$.

Identity Function on a Set

Definition

1_A is the **identity function** on A: $1_A(x) = x$ for all $x \in A$.

Theorem

For any $f : A \to B$, $f = 1_B \circ f = f \circ 1_A$

Proof.

Sketch of proof: Proving that the set f is equal to the set $f \circ 1_A$ and $1_B \circ f$. □

Note: if $\langle x, y \rangle \in f$, then $\langle x, y \rangle \in f$ and $\langle x, x \rangle \in 1_A$;
if $\langle x, y \rangle \in f \circ 1_A$, then there must be a $\langle t, y \rangle \in f$, and $\langle x, t \rangle \in 1_A$, then $t = x$, so $\langle x, y \rangle \in f$.

Identity Function on a Set

Definition

1_A is the **identity function** on A: $1_A(x) = x$ for all $x \in A$.

Theorem

For any $f : A \to B$, $f = 1_B \circ f = f \circ 1_A$

Proof.

Sketch of proof: Proving that the set f is equal to the set $f \circ 1_A$ and $1_B \circ f$. □

Note: if $\langle x, y\rangle \in f$, then $\langle x, y\rangle \in f$ and $\langle x, x\rangle \in 1_A$;
if $\langle x, y\rangle \in f \circ 1_A$, then there must be a $\langle t, y\rangle \in f$, and $\langle x, t\rangle \in 1_A$, then $t = x$, so $\langle x, y\rangle \in f$.

Invertible Function

The inverse relation of $f : A \to B$ is not necessarily a function, even though f is.

Example

Let $A = \{a, b, c\}$, $B = \{1, 2, 3\}$, $f = \{\langle a, 1\rangle, \langle b, 2\rangle, \langle c, 1\rangle\}$ is a function, but $f^{-1} = \{\langle 1, a\rangle, \langle 2, b\rangle, \langle 1, c\rangle\}$ is not a function.

Definition

$f : A \to B$ is called an **invertible function**, if its inverse relation, $f^{-1} : B \to A$ is also a function.

Example

$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(\langle i, j\rangle) = 2^i(2j + 1) - 1$ is a bijection

$$f^{-1}(2^i(2j + 1) - 1) = \langle i, j\rangle$$

Invertible Function

The inverse relation of $f : A \to B$ is not necessarily a function, even though f is.

Example

Let $A = \{a, b, c\}$, $B = \{1, 2, 3\}$, $f = \{\langle a, 1\rangle, \langle b, 2\rangle, \langle c, 1\rangle\}$ is a function, but $f^{-1} = \{\langle 1, a\rangle, \langle 2, b\rangle, \langle 1, c\rangle\}$ is not a function.

Definition

$f : A \to B$ is called an **invertible function**, if its inverse relation, $f^{-1} : B \to A$ is also a function.

Example

$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(\langle i, j\rangle) = 2^i(2j + 1) - 1$ is a bijection

$$f^{-1}(2^i(2j + 1) - 1) = \langle i, j\rangle$$

Invertible Function

The inverse relation of $f : A \to B$ is not necessarily a function, even though f is.

Example

Let $A = \{a, b, c\}$, $B = \{1, 2, 3\}$, $f = \{\langle a, 1\rangle, \langle b, 2\rangle, \langle c, 1\rangle\}$ is a function, but $f^{-1} = \{\langle 1, a\rangle, \langle 2, b\rangle, \langle 1, c\rangle\}$ is not a function.

Definition

$f : A \to B$ is called an **invertible function**, if its inverse relation, $f^{-1} : B \to A$ is also a function.

Example

$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(\langle i, j\rangle) = 2^i(2j + 1) - 1$ is a bijection

$$f^{-1}(2^i(2j + 1) - 1) = \langle i, j\rangle$$

Invertible Function

Theorem

$f : A \to B$ has an invert function if and only if f is a bijection.

Proof.

Sketch of proof:

$\Rightarrow$: If f is not an injection, then there must be $\langle y, x_1\rangle, \langle y, x_2\rangle \in f^{-1}$, and $x_1 \neq x_2$. On the other hand, if f is not a surjection, then there is at least one element in B, which has no image in A under f^{-1}. Both cases contradict to "$f^{-1} : B \to A$ is a function".

$\Leftarrow$: If f^{-1} is not a function, then, either there exist $\langle y, x_1\rangle, \langle y, x_2\rangle \in f^{-1}$, and $x_1 \neq x_2$, then f is not a injection, or there must be at least one element in B, which has no image in A under f^{-1}. Both cases contradict to "f is a bijection".

Invertible Function

Theorem

$f : A \to B$ has an invert function if and only if f is a bijection.

Proof.

Sketch of proof:

$\Rightarrow$: If f is not an injection, then there must be $\langle y, x_1\rangle, \langle y, x_2\rangle \in f^{-1}$, and $x_1 \neq x_2$. On the other hand, if f is not a surjection, then there is at least one element in B, which has no image in A under f^{-1}. Both cases contradict to "$f^{-1} : B \to A$ is a function".

$\Leftarrow$: If f^{-1} is not a function, then, either there exist $\langle y, x_1\rangle, \langle y, x_2\rangle \in f^{-1}$, and $x_1 \neq x_2$, then f is not a injection, or there must be at least one element in B, which has no image in A under f^{-1}. Both cases contradict to "f is a bijection".

Two Sets: Which is "larger"?

For finite sets, we can count the elements they contain, but how do we do with infinite sets?

Which is "larger", the set of natural number and the set of even number?

Equipotent Relation

Definition

The sets A and B are **equipotent** if there is a one-to-one correspondence from A to B.

- The notation: $A \approx B$, otherwise $A \not\approx B$
- If $A \approx B$, we can let each elements of A correspond to exactly one element of B, and vice versa.
- To prove $A \approx B$, find a one-to-one correspondence from A to B, any one.

Two equipotent sets can be regarded as with "the same size."

(Infinite) Countable Set

Definition

A set is **countable** if it is equipotent to some subset of the set of natural numbers.

- Which means: we can put all the elements of the set in a line, with the elements next to any specified element, both before and after, determined.
- The set of integer (including negative numbers) is equipotent to the set of natural number.

$$0, -1,\ 1, -2,\ 2, -3,\ 3, -4, \cdots$$

A set S is **finite**, iff. S is equipotent to some natural number n.

(Infinite) Countable Set

Definition

A set is **countable** if it is equipotent to some subset of the set of natural numbers.

- Which means: we can put all the elements of the set in a line, with the elements next to any specified element, both before and after, determined.
- The set of integer (including negative numbers) is equipotent to the set of natural number.

$$0, -1,\ 1, -2,\ 2, -3,\ 3, -4, \cdots$$

A set S is **finite**, iff. S is equipotent to some natural number n.

Finite Set and Infinite Set

Theorem

A set S is infinite, iff. existing a proper subset of S, say S', $S \approx S'$.

$\Rightarrow$: S must have a subset, $M = \{a_1, a_2, a_3, \cdots\}$, equipotent to the set of natural set (which means that the set of natural number is one of the "smallest" infinite set). Let $S' = S - \{a1\}$, define $f : S \to S'$ as follows:

$$f(x) = \begin{cases} a_{i+1} & \text{if } x = a_i \in M \\ x & x \in S - M \end{cases}$$

Obviously, this is a one-to-one correspondence, so, S is equipotent to one of its proper subset, S'.

$\Leftarrow$: If $|S| = n$, then for any S', a proper subset of S, if $|S'| = m$, then $m < n$, so, any injection form S' to S cannot be surjection.

Proving Equipotence

- $(0, 1)$ is equipotent to the set of all real number:
  One-to-one correspondence; $f : (0, 1) \to \mathbb{R}$:
  $f(x) = \tan(\pi x - \frac{\pi}{2})$
- For any two real numbers $a, b(a < b)$, $[0, 1] \approx [a, b]$:
  Correspondence: $f : [0, 1] \to [a, b]$: $f(x) = (b - a)x + a$
  (In fact, any two line segments with different length are equipotent.)
- Line and Plane: the set of points in a line, say $(0, 1)$, is equipotent to the set of points in a plane, say the square whose bottom left is $\langle 0, 0\rangle$ and top right $\langle 0, 0\rangle$.
  $\langle 0.x_1x_2x_3\cdots, 0.y_1y_2y_3\cdots\rangle \leftrightarrow 0.x_1y_1x_2y_2x_3y_3\cdots$
  (In fact, it is equipotent to the set of points in a space of any finite dimension.)

Proving Equipotence

- $(0, 1)$ is equipotent to the set of all real number:
  One-to-one correspondence; $f : (0, 1) \to \mathbb{R}$:
  $f(x) = \tan(\pi x - \frac{\pi}{2})$
- For any two real numbers $a, b(a < b)$, $[0, 1] \approx [a, b]$:
  Correspondence: $f : [0, 1] \to [a, b]$: $f(x) = (b - a)x + a$
  (In fact, any two line segments with different length are equipotent.)
- Line and Plane: the set of points in a line, say $(0, 1)$, is equipotent to the set of points in a plane, say the square whose bottom left is $\langle 0, 0\rangle$ and top right $\langle 0, 0\rangle$.
  $\langle 0.x_1x_2x_3\cdots, 0.y_1y_2y_3\cdots\rangle \leftrightarrow 0.x_1y_1x_2y_2x_3y_3\cdots$
  (In fact, it is equipotent to the set of points in a space of any finite dimension.)

Proving Equipotence

- $(0, 1)$ is equipotent to the set of all real number:
  One-to-one correspondence; $f : (0, 1) \to \mathbb{R}$:
  $f(x) = \tan(\pi x - \frac{\pi}{2})$
- For any two real numbers $a, b(a < b)$, $[0, 1] \approx [a, b]$:
  Correspondence: $f : [0, 1] \to [a, b]$: $f(x) = (b - a)x + a$
  (In fact, any two line segments with different length are equipotent.)
- Line and Plane: the set of points in a line, say $(0, 1)$, is equipotent to the set of points in a plane, say the square whose bottom left is $\langle 0, 0\rangle$ and top right $\langle 0, 0\rangle$.
  $\langle 0.x_1x_2x_3\cdots, 0.y_1y_2y_3\cdots\rangle \leftrightarrow 0.x_1y_1x_2y_2x_3y_3\cdots$
  (In fact, it is equipotent to the set of points in a space of any finite dimension.)

Proving Equipotence

- $(0, 1)$ is equipotent to the set of all real number:
  One-to-one correspondence; $f : (0, 1) \to \mathbb{R}$:
  $f(x) = \tan(\pi x - \frac{\pi}{2})$
- For any two real numbers $a, b(a < b)$, $[0, 1] \approx [a, b]$:
  Correspondence: $f : [0, 1] \to [a, b]$: $f(x) = (b - a)x + a$

  (In fact, any two line segments with different length are equipotent.)
- Line and Plane: the set of points in a line, say $(0, 1)$, is equipotent to the set of points in a plane, say the square whose bottom left is $\langle 0, 0\rangle$ and top right $\langle 0, 0\rangle$.
  $\langle 0.x_1x_2x_3\cdots, 0.y_1y_2y_3\cdots\rangle \leftrightarrow 0.x_1y_1x_2y_2x_3y_3\cdots$

  (In fact, it is equipotent to the set of points in a space of any finite dimension.)

Proving Equipotence

- $(0, 1)$ is equipotent to the set of all real number:
  One-to-one correspondence; $f : (0, 1) \to \mathbb{R}$:
  $f(x) = \tan(\pi x - \frac{\pi}{2})$
- For any two real numbers $a, b(a < b)$, $[0, 1] \approx [a, b]$:
  Correspondence: $f : [0, 1] \to [a, b]$: $f(x) = (b - a)x + a$
  (In fact, any two line segments with different length are equipotent.)
- Line and Plane: the set of points in a line, say $(0, 1)$, is equipotent to the set of points in a plane, say the square whose bottom left is $\langle 0, 0\rangle$ and top right $\langle 0, 0\rangle$.
  $\langle 0.x_1x_2x_3\cdots, 0.y_1y_2y_3\cdots\rangle \leftrightarrow 0.x_1y_1x_2y_2x_3y_3\cdots$
  (In fact, it is equipotent to the set of points in a space of any finite dimension.)

Proving Equipotence

- $(0, 1)$ is equipotent to the set of all real number:
  One-to-one correspondence; $f : (0, 1) \to \mathbb{R}$:
  $f(x) = \tan(\pi x - \frac{\pi}{2})$
- For any two real numbers $a, b(a < b)$, $[0, 1] \approx [a, b]$:
  Correspondence: $f : [0, 1] \to [a, b]$: $f(x) = (b - a)x + a$

  (In fact, any two line segments with different length are equipotent.)
- Line and Plane: the set of points in a line, say $(0, 1)$, is equipotent to the set of points in a plane, say the square whose bottom left is $\langle 0, 0\rangle$ and top right $\langle 0, 0\rangle$.
  $\langle 0.x_1x_2x_3\cdots, 0.y_1y_2y_3\cdots\rangle \leftrightarrow 0.x_1y_1x_2y_2x_3y_3\cdots$

  (In fact, it is equipotent to the set of points in a space of any finite dimension.)

Cantor's Theorem

Theorem

A set S cannot be equipotent to its power set, that is, $A \not\approx P(A)$

Proof.

Sketch of the proof: Let g be a function from A to $P(A)$, define a set B as follows:

$$B = \{x | x \in A, \text{ but } x \notin g(x)\}$$

So, $B \in P(A)$, but it is impossible that for some $x \in A$, such that $g(x) = B$, otherwise, $x \in B$ iff. $x \notin B$. So, g cannot be surjection, nor one-to-one correspondence, of course. □

Cantor's Theorem

Theorem

A set S cannot be equipotent to its power set, that is, $A \not\approx P(A)$

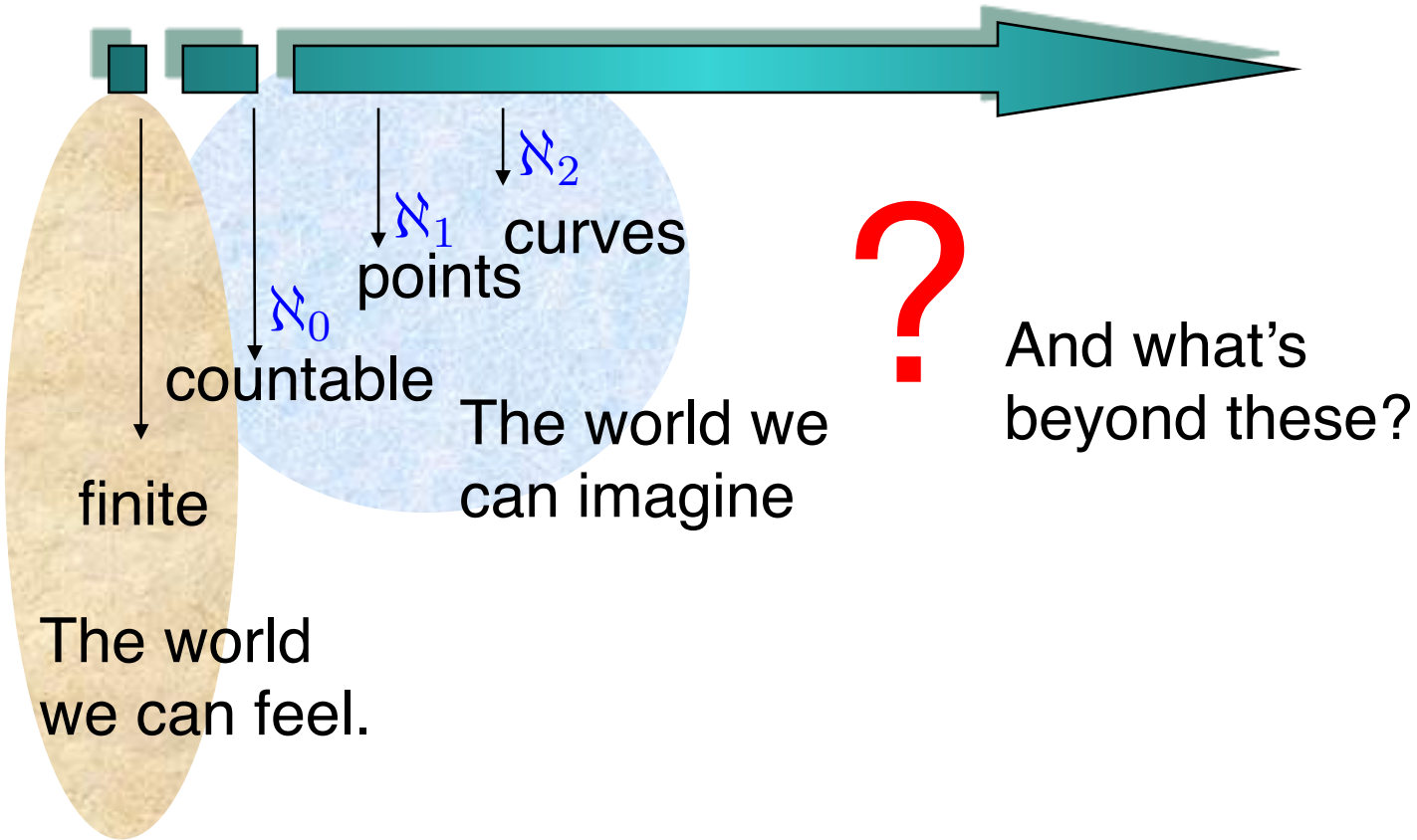
Proof.

Sketch of the proof: Let g be a function from A to $P(A)$, define a set B as follows:

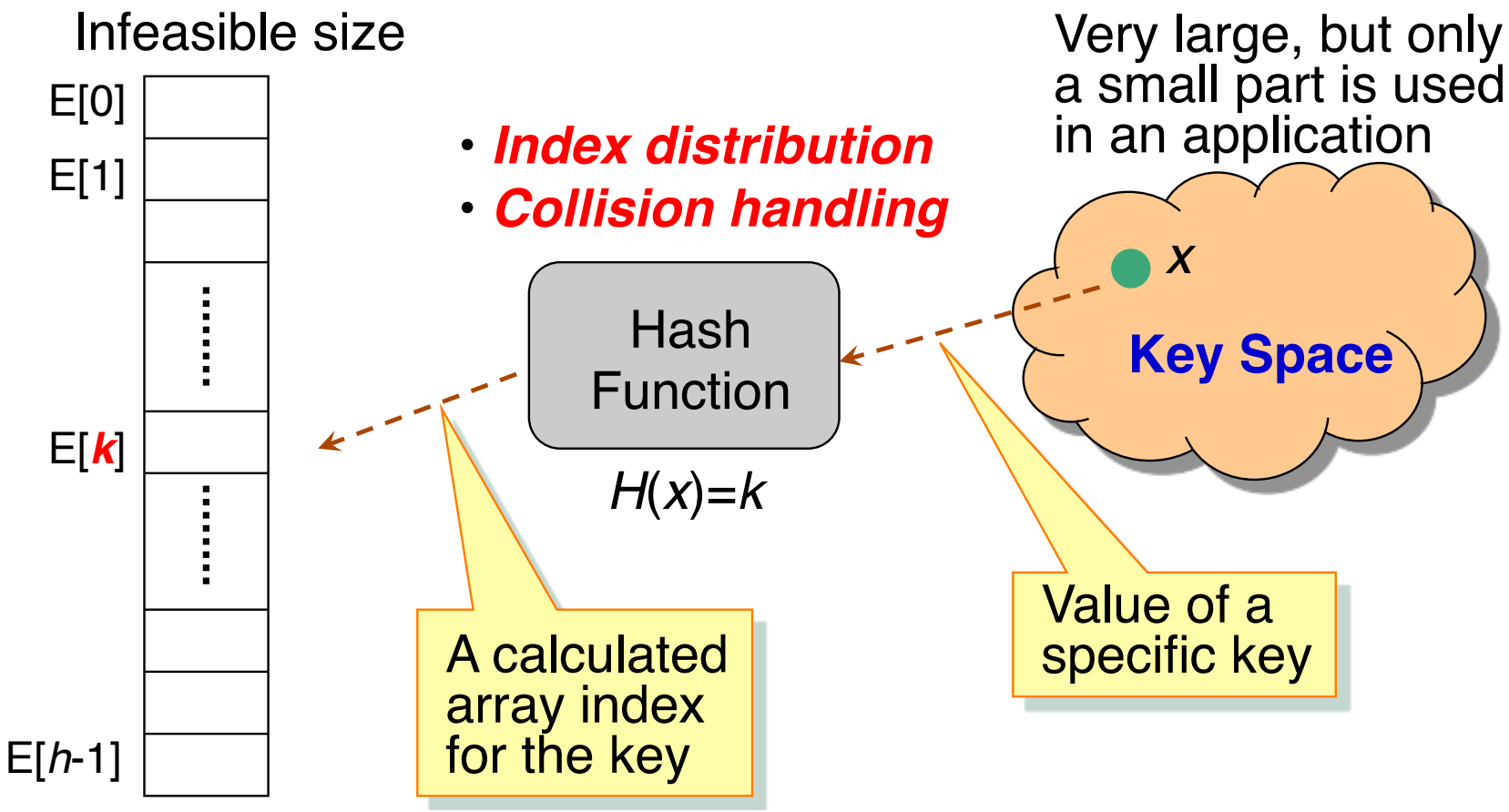
$$B = \{x | x \in A, \text{ but } x \notin g(x)\}$$

So, $B \in P(A)$, but it is impossible that for some $x \in A$, such that $g(x) = B$, otherwise, $x \in B$ iff. $x \notin B$. So, g cannot be surjection, nor one-to-one correspondence, of course. □

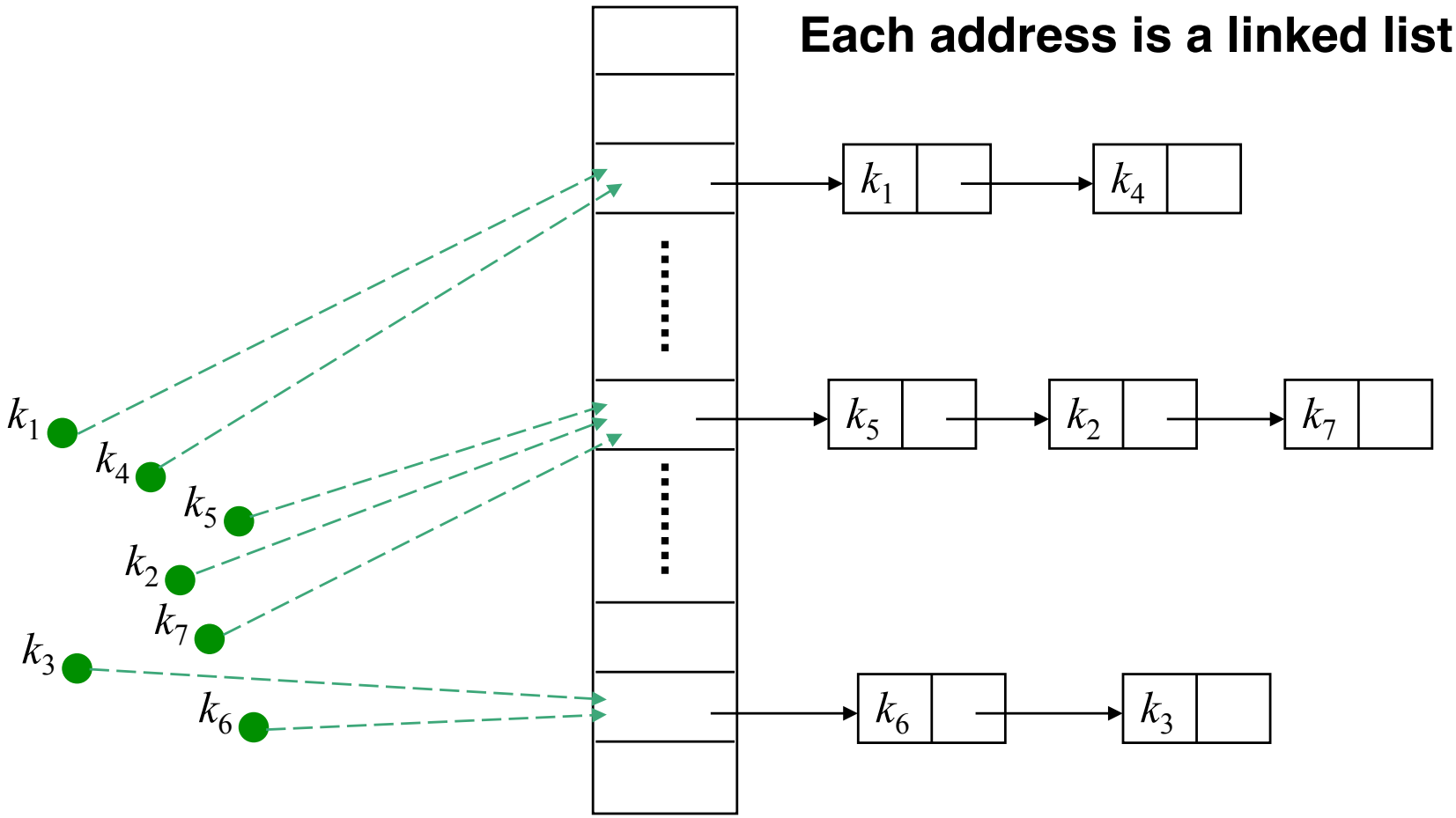
Size of Set – Cardinality



Hashing: the Idea



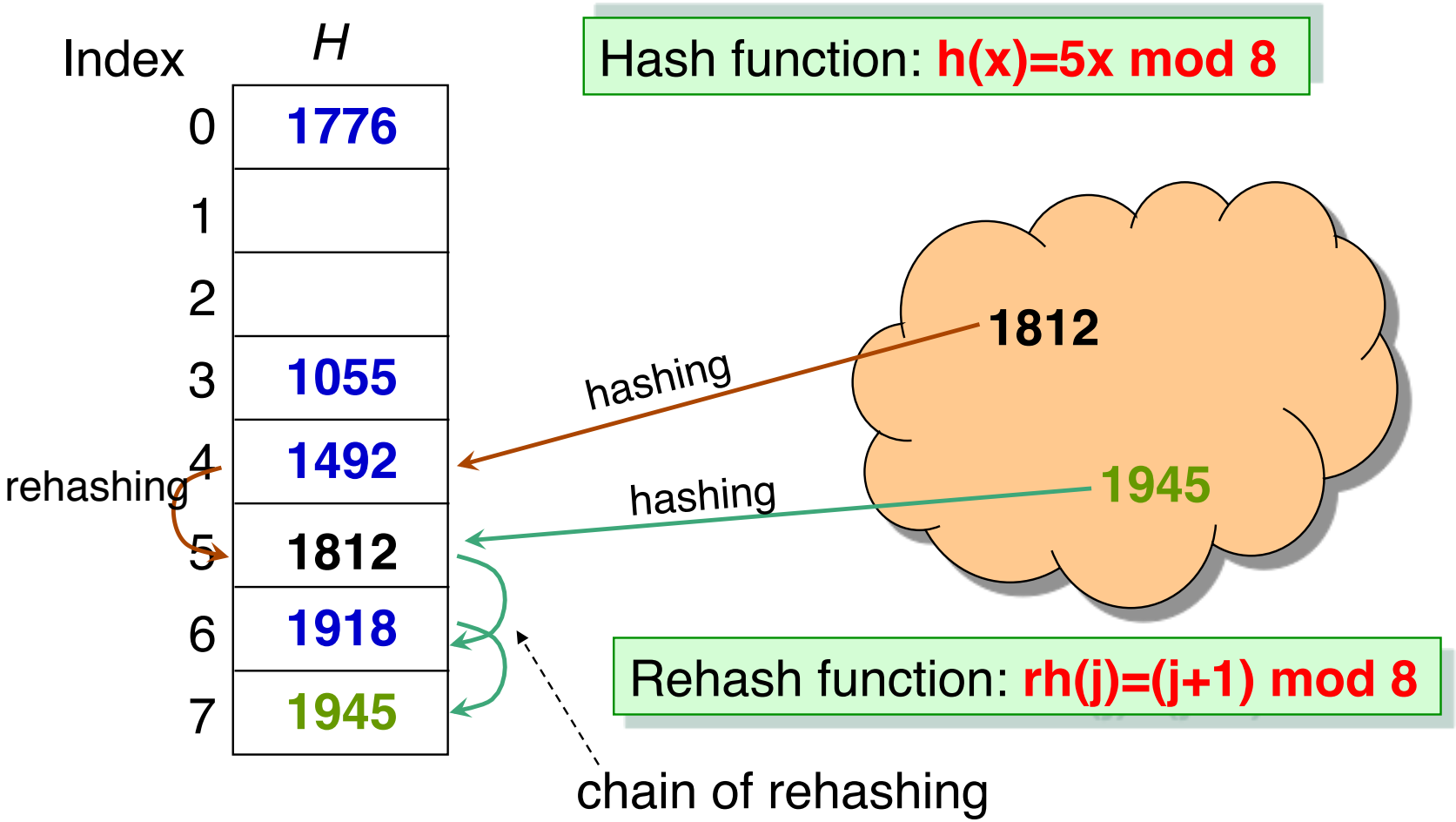
Collision Handling: Closed Address



Collision Handling: Open Address

- All elements are stored in the hash table, no linked list is used. So, α, the load factor, can not be larger than 1.
- Collision is settled by "rehashing": a function is used to get a new hashing address for each collided address, i.e., the hash table slots are probed successively, until a valid location is found.
- The probe sequence can be seen as a permutation of $(0, 1, 2, \cdots, h-1)$.

Linear Probing: an Example



Hashing Function

- A good hash function satisfies the assumption of simple uniform hashing.
- Heuristic hashing functions
  - The division method: $h(k) = k \bmod m$
  - The multiplication method: $h(k) = \lfloor m(kA \bmod 1) \rfloor$, $(0 < A < 1)$
- No single function can avoid the worst case, so, "Universal hashing" is proposed.
- Rich resource about hashing function: Gonnet and Baeza-Yates: *Handbook of Algorithms and Data Structures*, Addison-Wesley, 1991

Hashing Function

- A good hash function satisfies the assumption of simple uniform hashing.
- Heuristic hashing functions
  - The division method: $h(k) = k \bmod m$
  - The multiplication method: $h(k) = \lfloor m(kA \bmod 1) \rfloor$, $(0 < A < 1)$
- No single function can avoid the worst case, so, "Universal hashing" is proposed.
- Rich resource about hashing function: Gonnet and Baeza-Yates: *Handbook of Algorithms and Data Structures*, Addison-Wesley, 1991

Hashing Function

- A good hash function satisfies the assumption of simple uniform hashing.
- Heuristic hashing functions
  - The division method: $h(k) = k \bmod m$
  - The multiplication method: $h(k) = \lfloor m(kA \bmod 1) \rfloor$, $(0 < A < 1)$
- No single function can avoid the worst case, so, "Universal hashing" is proposed.
- Rich resource about hashing function: Gonnet and Baeza-Yates: *Handbook of Algorithms and Data Structures*, Addison-Wesley, 1991

Hashing Function

- A good hash function satisfies the assumption of simple uniform hashing.
- Heuristic hashing functions
  - The division method: $h(k) = k \bmod m$
  - The multiplication method: $h(k) = \lfloor m(kA \bmod 1) \rfloor$, $(0 < A < 1)$
- No single function can avoid the worst case, so, "Universal hashing" is proposed.
- Rich resource about hashing function: Gonnet and Baeza-Yates: *Handbook of Algorithms and Data Structures*, Addison-Wesley, 1991

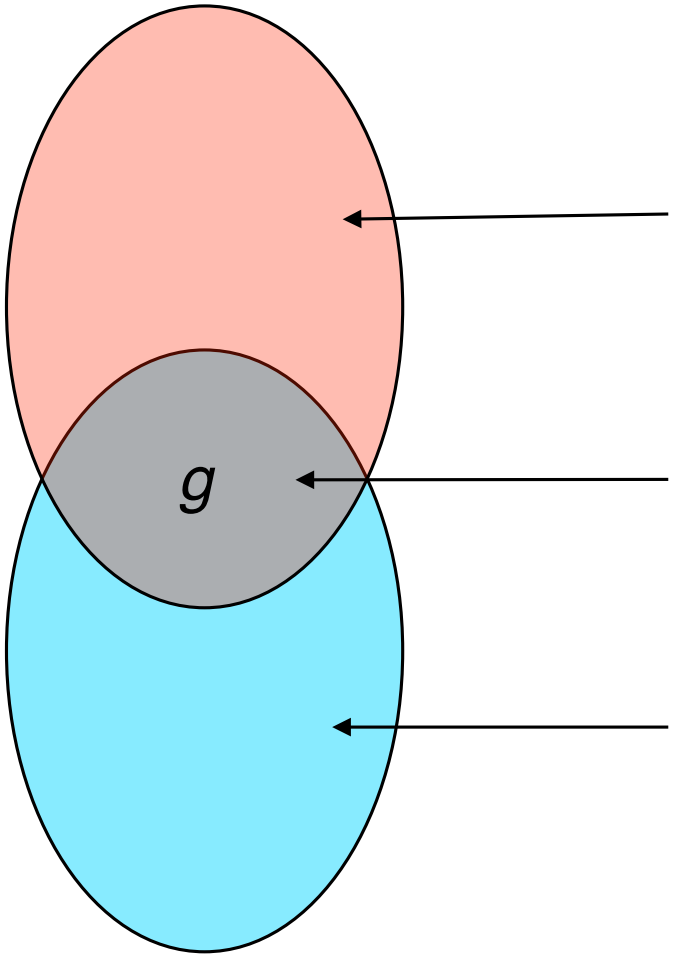
Hashing Function

- A good hash function satisfies the assumption of simple uniform hashing.
- Heuristic hashing functions
  - The division method: $h(k) = k \bmod m$
  - The multiplication method: $h(k) = \lfloor m(kA \bmod 1) \rfloor$, $(0 < A < 1)$
- No single function can avoid the worst case, so, "Universal hashing" is proposed.
- Rich resource about hashing function: Gonnet and Baeza-Yates: *Handbook of Algorithms and Data Structures*, Addison-Wesley, 1991

Hashing Function

- A good hash function satisfies the assumption of simple uniform hashing.
- Heuristic hashing functions
  - The division method: $h(k) = k \bmod m$
  - The multiplication method: $h(k) = \lfloor m(kA \bmod 1) \rfloor$, $(0 < A < 1)$
- No single function can avoid the worst case, so, "Universal hashing" is proposed.
- Rich resource about hashing function: Gonnet and Baeza-Yates: *Handbook of Algorithms and Data Structures*, Addison-Wesley, 1991

Relative Growth Rate



$\Omega(g)$: functions that grow at least as fast as g

$\Theta(g)$: functions that grow at the same rate as g

$O(g)$: functions that grow no faster as g

The Set "Big Oh"

Definition

Giving $g : \mathbb{N} \to \mathbb{R}^+$, then $O(g)$ is the set of $f : \mathbb{N} \to \mathbb{R}^+$, such that for some $c \in \mathbb{R}^+$ and some $n_0 \in \mathbb{N}$, $f(n) \leq c \cdot g(n)$ for all $n \geq n_0$.

A function $f \in O(g)$ if $\lim_{n\to\infty} \frac{f(n)}{g(n)} = c < \infty$

Note: c may be zero. In that case, $f \in o(g)$, "little Oh"

Example

let $f(n) = n^2, g(n) = n \lg n$, then:

$f \notin O(g)$, since

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = \lim_{n\to\infty} \frac{n^2}{n \lg n} = \lim_{n\to\infty} \frac{n}{\lg n} = \lim_{n\to\infty} \frac{1}{\frac{1}{n \ln 2}} = \infty$$

$g \in O(f)$, since $\lim_{n\to\infty} \frac{g(n)}{f(n)} = 0$

The Set "Big Oh"

Definition

Giving $g : \mathbb{N} \to \mathbb{R}^+$, then $O(g)$ is the set of $f : \mathbb{N} \to \mathbb{R}^+$, such that for some $c \in \mathbb{R}^+$ and some $n_0 \in \mathbb{N}$, $f(n) \leq c \cdot g(n)$ for all $n \geq n_0$.

A function $f \in O(g)$ if $\lim\limits_{n\to\infty} \dfrac{f(n)}{g(n)} = c < \infty$

Note: c may be zero. In that case, $f \in o(g)$, "little Oh"

Example

let $f(n) = n^2, g(n) = n \lg n$, then:

$f \notin O(g)$, since

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = \lim_{n\to\infty} \frac{n^2}{n \lg n} = \lim_{n\to\infty} \frac{n}{\lg n} = \lim_{n\to\infty} \frac{1}{\frac{1}{n \ln 2}} = \infty$$

$g \in O(f)$, since $\lim\limits_{n\to\infty} \dfrac{g(n)}{f(n)} = 0$

The Set "Big Oh"

Definition

Giving $g : \mathbb{N} \to \mathbb{R}^+$, then $O(g)$ is the set of $f : \mathbb{N} \to \mathbb{R}^+$, such that for some $c \in \mathbb{R}^+$ and some $n_0 \in \mathbb{N}$, $f(n) \leq c \cdot g(n)$ for all $n \geq n_0$.

A function $f \in O(g)$ if $\lim\limits_{n\to\infty} \dfrac{f(n)}{g(n)} = c < \infty$

Note: c may be zero. In that case, $f \in o(g)$, "little Oh"

Example

let $f(n) = n^2, g(n) = n \lg n$, then:

$f \notin O(g)$, since

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = \lim_{n\to\infty} \frac{n^2}{n \lg n} = \lim_{n\to\infty} \frac{n}{\lg n} = \lim_{n\to\infty} \frac{1}{\frac{1}{n \ln 2}} = \infty$$

$g \in O(f)$, since $\lim\limits_{n\to\infty} \dfrac{g(n)}{f(n)} = 0$

The Sets Ω and Θ

Definition

Giving $g : \mathbb{N} \to \mathbb{R}+$, then $\Omega(g)$ is the set of $f : \mathbb{N} \to \mathbb{R}^+$, such that for some $c \in \mathbb{R}^+$ and some $n_0 \in N$, $f(n) \geq c \cdot g(n)$ for all $n \geq n_0$.

A function $f \in \Omega(g)$ if $\lim_{n\to\infty} \frac{f(n)}{g(n)} > 0$.

Note: the limit may be infinity.

Definition

Giving $g : \mathbb{N} \to \mathbb{R}^+$, then $\Theta(g) = O(g) \cap \Omega(g)$

A function $f \in \Theta(g)$ if $lim_{n\to\infty} \frac{f(n)}{g(n)} = c$, $0 < c < \infty$.

The Sets Ω and Θ

Definition

Giving $g : \mathbb{N} \to \mathbb{R}+$, then $\Omega(g)$ is the set of $f : \mathbb{N} \to \mathbb{R}^+$, such that for some $c \in \mathbb{R}^+$ and some $n_0 \in N$, $f(n) \geq c \cdot g(n)$ for all $n \geq n_0$.

A function $f \in \Omega(g)$ if $\lim_{n\to\infty} \frac{f(n)}{g(n)} > 0$.

Note: the limit may be infinity.

Definition

Giving $g : \mathbb{N} \to \mathbb{R}^+$, then $\Theta(g) = O(g) \cap \Omega(g)$

A function $f \in \Theta(g)$ if $lim_{n\to\infty} \frac{f(n)}{g(n)} = c$, $0 < c < \infty$.

How Functions Grow

Algorithm	1	2	3	4	5
Time function(ms)	$33n$	$46n \ln n$	$13n^2$	$3.4n^3$	2^n
Input size n	Solution time				
10	0.00033s	0.0015s	0.0013s	0.0034s	0.001s
100	0.0033s	0.03s	0.13s	3.4s	4×10^{16} yr.
1,000	0.033s	0.45s	13s	0.94 hr.	
10,000	0.33s	6.1s	22 min.	39 days	
100,000	3.3s	1.3 min.	1.5 days	108 yr.	
Time allowed	Maximum solvable input size (approx.)				
1 second	30,000	2,000	280	67	20
1 minute	1,800,000	82,000	2,200	260	26

Increasing Computer Speed

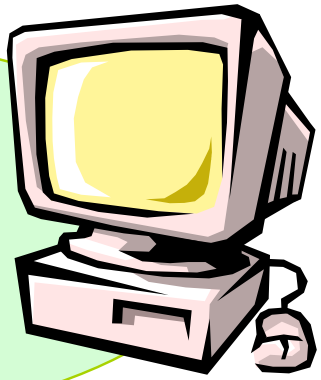
Number of steps performed on input of size n $f(n)$	Maximum feasible input size s	Maximum feasible input size in t times as much time s_{new}
$\lg n$	s_1	s_1^t
n	s_2	$t \cdot s_2$
n^2	s_3	$\sqrt{t} \cdot s_3$
2^n	s_4	$\lg t + s_4$

Sorting a Array of 1 Million Numbers

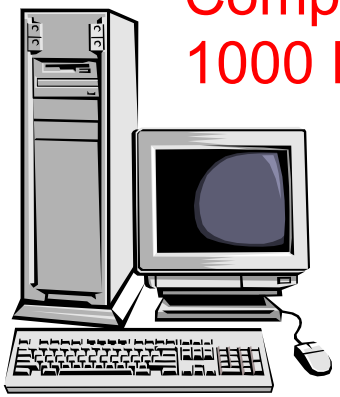
Using ***merge sort***,
taking time $50n\log n$:

100 seconds!

Computer B
10 Mips



Computer A
1000 Mips



Using ***insertion sort***, taking time $2n^2$:

2000 seconds!

Complexity Class

Let S be a set of $f : \mathbb{N} \to \mathbb{R}^+$ under consideration, define the relation $\sim$ on S as following: $f \sim g$ iff. $f \in \Theta(g)$, then, $\sim$ is an equivalence.

Each set $\Theta(g)$ is an equivalence class, called complexity class.

We usually use the simplest element as possible as the representative, so, $\Theta(n)$, $\Theta(n^2)$, etc.

Comparison of Often Used Orders

- The log function grows more slowly than any positive power of n

$$\lg n \in o(n^{\alpha}) \text{ for any } \alpha > 0$$

- The power of n grows more slowly than any exponential function with base greater than 1

$$n^{k} \in o(c^{n}) \text{ for any } c > 1$$

(The commonly seen base is 2)

More rules for Determining the Θ-Class

- $\Theta(1)$ functions are constant and have 0 growth, the slowest.
- $\Theta(n^a)$ is lower than $\Theta(n^b)$ if and only if $0 < a < b$.
- $\Theta(a^n)$ is lower than $\Theta(b^n)$ if and only if $0 < a < b$.
- If constant r is not zero, then $\Theta(rf) = \Theta(f)$ for any function f.
- If h is a nonzero function and $\Theta(f)$ is lower than (or the same as) $\Theta(g)$, then $\Theta(fh)$ is lower than (or the same as) $\Theta(gh)$.
- if $\Theta(f)$ is lower than $\Theta(g)$, then $\Theta(f + g) = \Theta(g)$.

Order of Common Sums

- $\sum_{i=1}^{n} i^d \in \Theta\left(n^{d+1}\right)$
- $\sum_{i=a}^{b} r^i \in \Theta\left(r^k\right)$, r^k is the largest term in the sum
- $\sum_{i=1}^{n} \log(i) \in \Theta(n \log n)$
- $\sum_{i=1}^{n} i^d \log(i) \in \Theta\left(n^{d+1} \log(n)\right)$

Permutation Function

Definition

A bijection from a set A to itself is called a **permutation** of A.

Denotation: $p = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ p(a_1) & p(a_2) & \cdots & p(a_n) \end{pmatrix}$

Example

$S = \{1, 2, 3\}$, there are 6 different permutations of S:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \delta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \epsilon = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Permutation Function

Definition

A bijection from a set A to itself is called a **permutation** of A.

Denotation: $p = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ p(a_1) & p(a_2) & \cdots & p(a_n) \end{pmatrix}$

Example

$S = \{1, 2, 3\}$, there are 6 different permutations of S:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \delta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \epsilon = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Cyclic Permutation and Transposition

Definition

If p is a permutation of $S = \{1, 2, \cdots, n\}$, and
$p(i_1) = i_2$, $p(i_2) = i_3$, $\cdots$, $p(i_{k-1}) = i_k$, $p(i_k) = i_1$,
for all other $x \in S$, $p(x) = x$,
then p is called a **cyclic permutation** of S, when $k = 2$, p is also called a **transposition**.

Denotation: $(i_1 i_2 \cdots i_k)$

Example

6 permutations of $S = \{1, 2, 3\}$:
$e = (1)$; $\alpha = (123)$; $\beta = (132)$; $\gamma = (23)$; $\delta = (13)$; $\epsilon = (12)$

Disjoint Cyclic Permutations

- Given two cyclic permutations of S:
  $p = (i_1 i_2 \cdots i_k)$, $q = (j_1 j_2 \cdots j_s)$,
  if $\{i_1, i_2, \cdots, i_k\} \cap \{j_1, j_2, \cdots, j_s\} = \emptyset$,
  then p and q are **disjoint**.

- If p and q are disjoint, then $p \circ q = q \circ p$
  For any $x \in S$, there are three cases:
  1. $x \in \{i_1, i_2, \cdots, i_k\}$;
  2. $x \in \{j_1, j_2, \cdots, j_s\}$;
  3. $x \in S - (\{i_1, i_2, \cdots, i_k\} \cup \{j_1, j_2, \cdots, j_s\})$

  it is easy to see $(p \circ q)(x) = (q \circ p)(x)$ in all the three cases.

Permutation as Product of Cycles

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 3 & 8 & 7 & 6 & 1 & 4 \end{pmatrix} = (157) \circ (48)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 8 & 1 & 4 & 6 & 7 \end{pmatrix} = (1235) \circ (4876)$$

Permutation as Product of Transpositions

Theorem

Every cycle $p = (i_1 i_2 \cdots i_k)$ *can be represented as a product of* $k-1$ *transpositions* $(i_1 i_k) \circ (i_1 i_{k-1}) \circ \cdots \circ (i_1 i_2)$

The order cannot be changed.

Proof.

Proof by induction on k: $k = 2$ is trivial. Considering $p = (i_1 i_2 \cdots i_k i_{k+1})$, we need only to prove that $p = (i_1 i_{k+1}) \circ (i_1 i_2 \cdots i_k)$. There are four cases for any $x \in A$, $p(x) = (i_1 i_{k+1})(i_1 i_2 \cdots i_k)(x)$

1. $x \in \{i_1, i_2, \cdots, i_{k-1}\}$
2. $x = i_k$
3. $x = i_{k+1}$
4. otherwise

Permutation as Product of Cycles

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 3 & 8 & 7 & 6 & 1 & 4 \end{pmatrix} = (157) \circ (48) = (17) \circ (15) \circ (48)$$

Odd

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 8 & 1 & 4 & 6 & 7 \end{pmatrix} = (1235) \circ (4876)$$

$$= (15) \circ (13) \circ (12) \circ (46) \circ (47) \circ (48)$$

Even

Home Assignments

To be checked

- Ex. 5.1: 5-8, 11-15, 29-31, 33-34, 40-41
- Ex. 5.2: 7-8, 18, 20, 28-29,
- Ex. 5.3: 11-13, 20-29
- Ex. 5.4: 12-16, 20, ,26, 28-30, 37-39

The End