Functions

Lecture 6

Discrete Mathematical Structures

Functions

- Part I: Basics of Functions
  - Function as a class of special relations
  - Types of functions
  - Function and Comparison of Set Size
  - Permutation: bijection on one set
- Part II: Functions and Computer Science
  - Commonly used function in computer applications
  - Growth of functions

Definition of Function

- Definition: Let A and B be nonempty sets. A ***function*** f from A to B, which is denoted $f{:}A\to B$, is a relation from A to B such that for each $a\in \mathrm{Dom}(A)$, $f(a)$ 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.

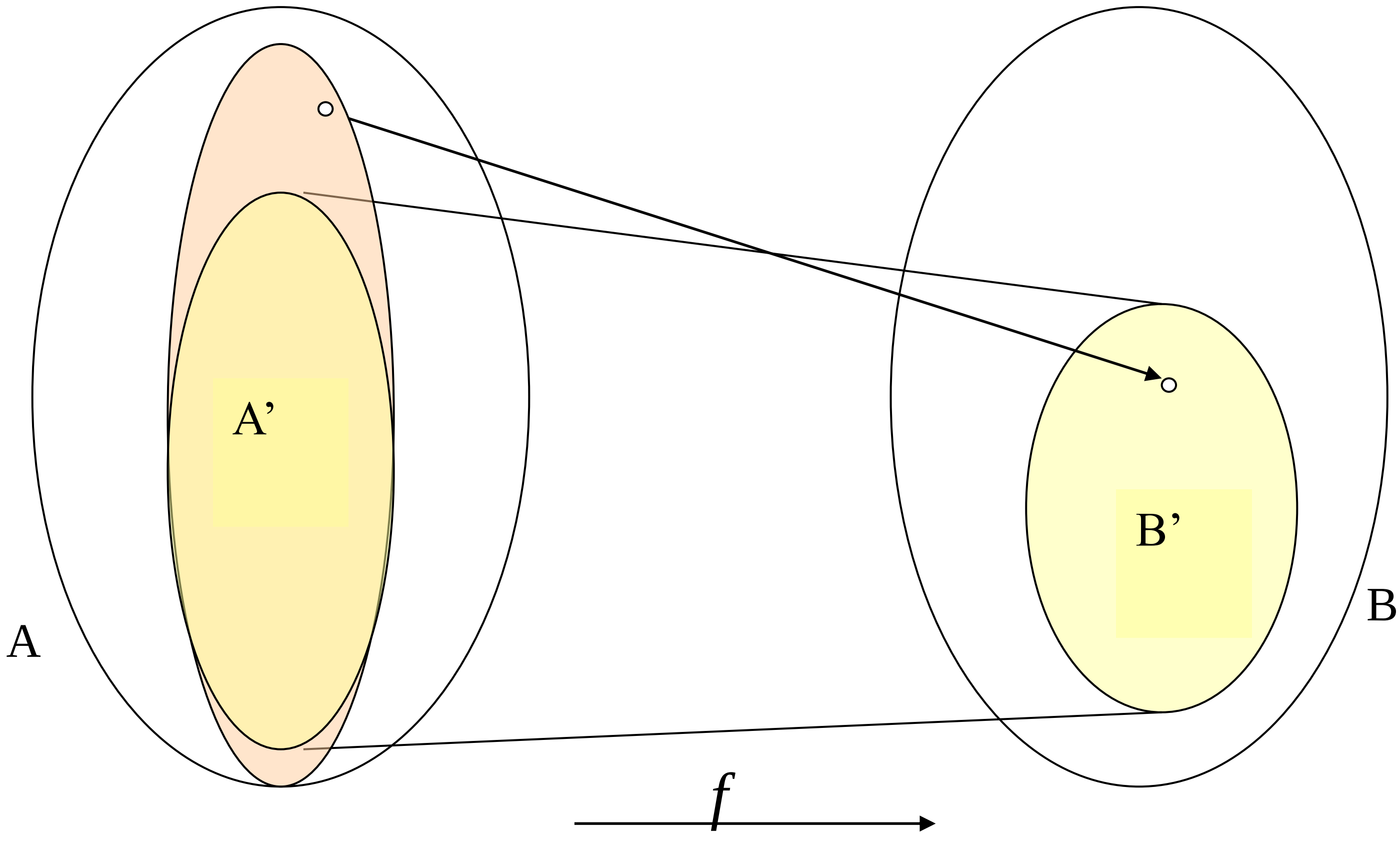
Image and counterimage

- Let f:$A\rightarrow B$, $A'\subseteq A$, 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
- Let $B'\subseteq B$, then $f^{-1}(B')=\{x|x\in A,\ f(x)\in B'\}$ is called the counter-image 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→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 (one-to-one)
  - f:A→B is 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: Examples

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

Characteristic Function of Set

- 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. $x \in A$

- The one-to-one correspondence between
  - $\rho(U)$, the power set of U,
  - All characteristic functions of A, $\chi_A : U \to \{0,1\}$

Natural Function

- R is an equivalence relation on set A,
  - g : A$\rightarrow$A/R, for all a$\in$A, $g(a)=R(\mathrm{a})$,
  - 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 $g(x)=R(\mathrm{x})$

Images of Union and Intersection

- Given f: $A \to B$, and X, Y are subsets of A, then:
  - $f(X \cup Y) = f(X) \cup f(Y)$
  - $f(X \cap Y) \subseteq f(X) \cap f(Y)$

Counterexample for $f(X) \cap f(Y) \subseteq f(X \cap Y)$

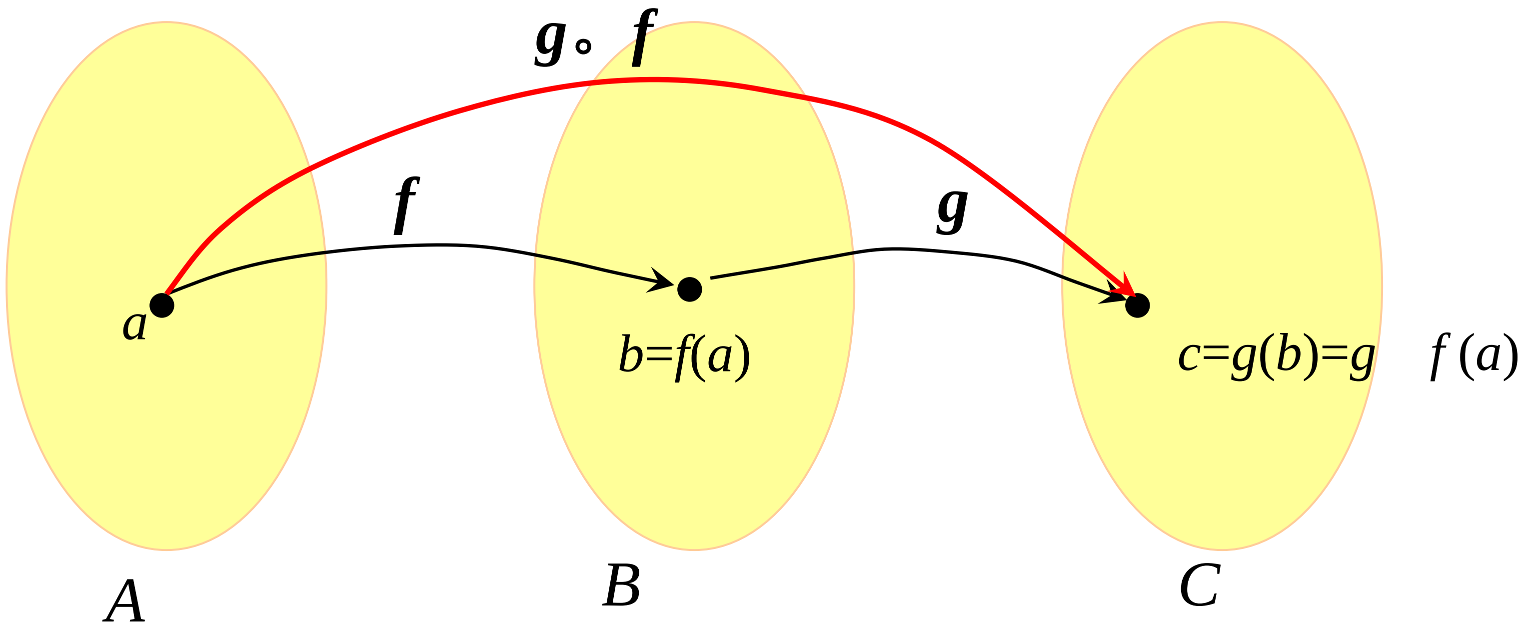
$a \in X$, but $a \notin Y$, and $b \in Y$, but $b \notin X$
However, $f(a) = f(b) = c$, then: $c \in f(X) \cap f(Y)$
but, maybe $c \notin f(X \cap Y)$

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
  - Suppose $f:A\rightarrow B$, $g:B\rightarrow C$, $g\circ f$ 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.

Composition of Functions



Associative Law

- The composition of function is simply the composition of relation, so it is an associative operation.

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

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

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.
- 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, $g\circ f(x)=y$.

But…

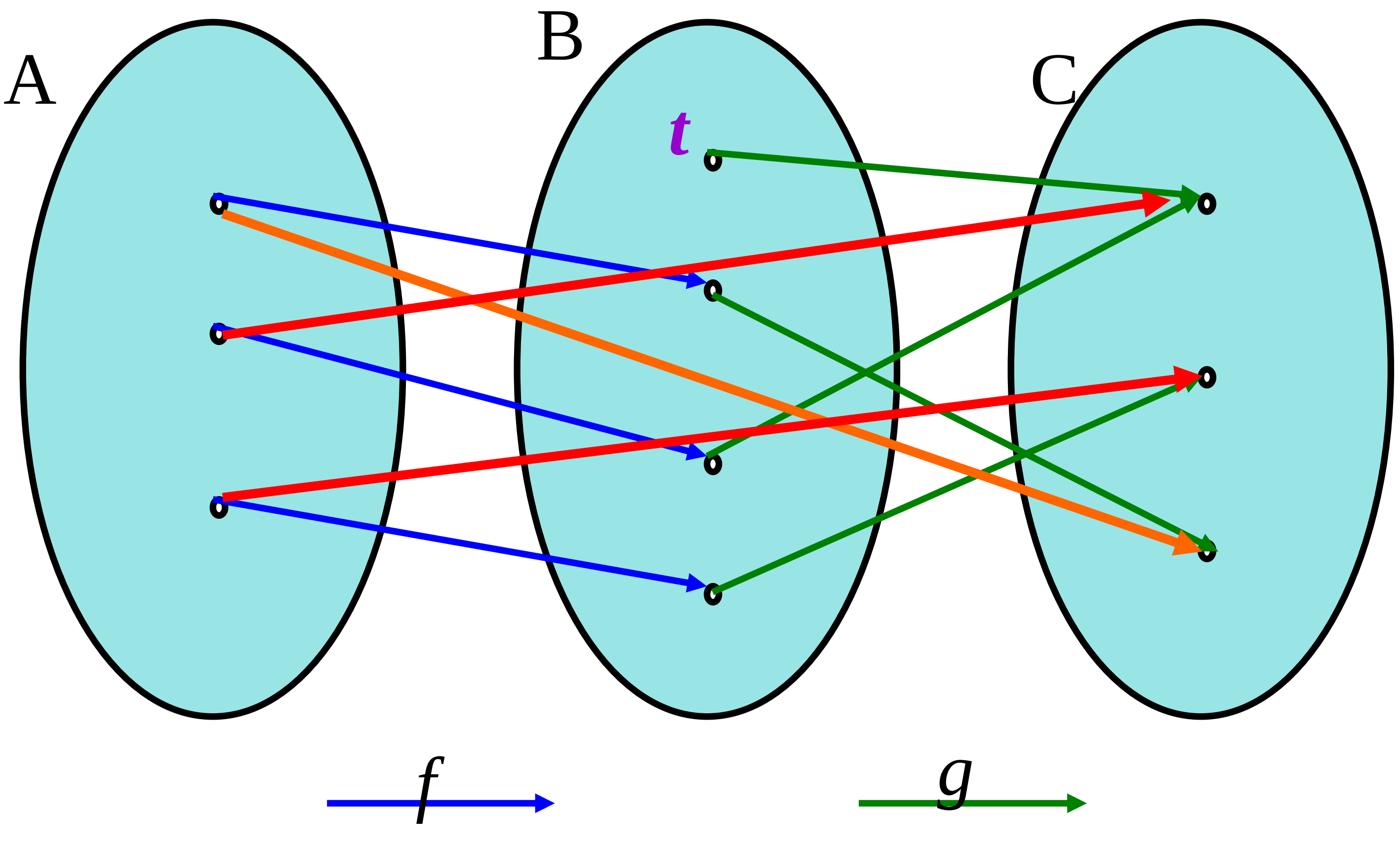
- If $g \circ f$ is a surjection， can it be derived that f and g are both surjections as well？
  - Obviously， g ***must be*** a surjection.

- 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 $g(B\text{-}t)=C$, $g \circ f$ is still a surjection.

Composition is a Surjection



Composition of Injections

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

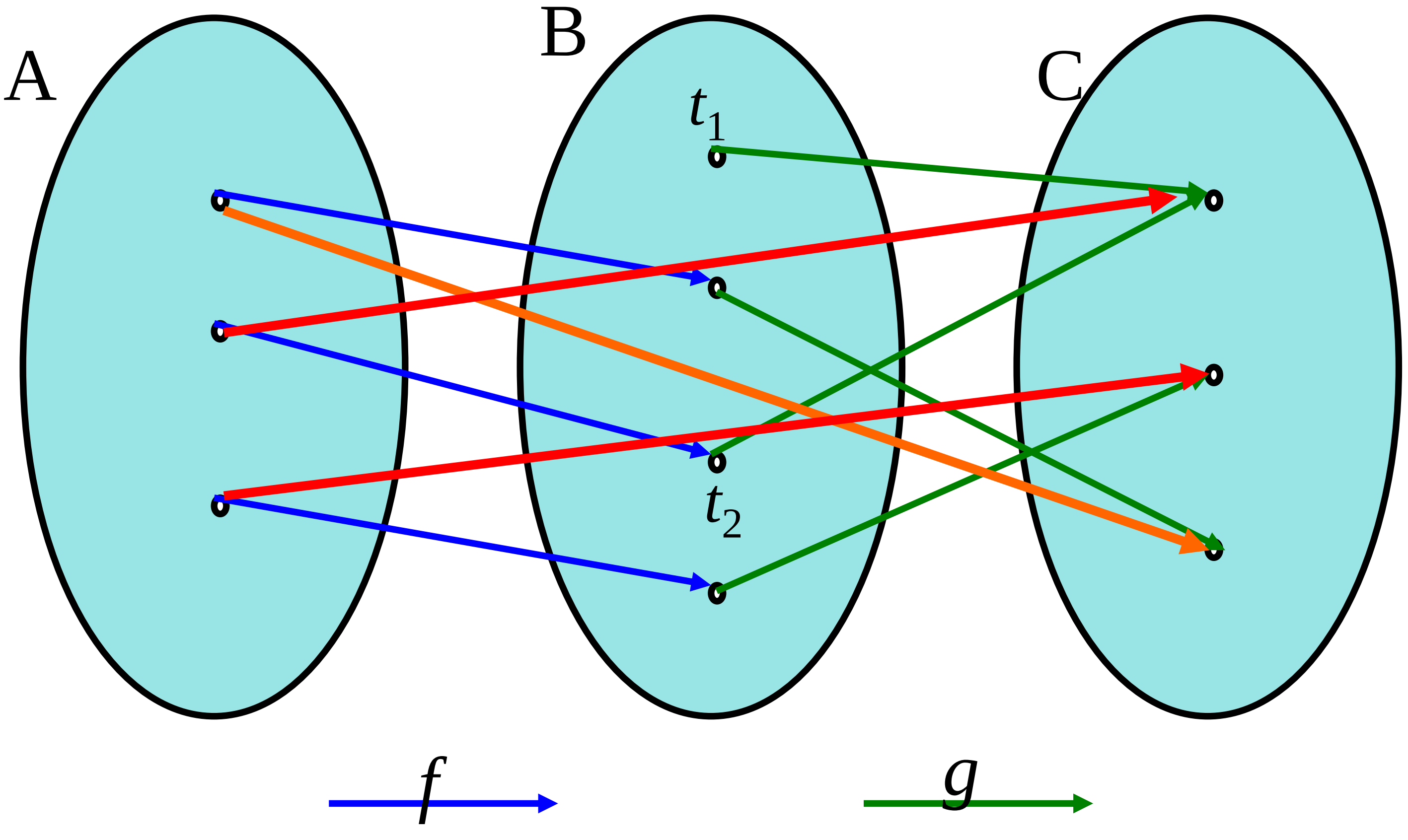
  If $t_1 \neq t_2$, then g is **not** a injection.

But…

- 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

- 1_A is the identity function on A

$$1_A(x)=x \text{ for all } x\in A.$$

- For any $f:A\to B$, $f=1_B\circ f=f\circ 1_A$
- Sketch of proof:

Proving that f is equal to $f\circ 1_A$ and $1_B\circ f$

- if $<x,y>\in f$, then $<x,y>\in f$ and $<x,x>\in 1_A$
- if $<x,y>\in f\circ 1_A$, then $<t,y>\in f$ and $<x,t>\in 1_A$, $t=x$, so $<x,y>\in f$.

Invertible Function

- The inverse relation of $f: A \rightarrow B$ is not necessarily a function, even though f is.
  - Examples: (Let A={a,b,c}, B={1,2,3})

    $f = \{<a,1>, <b,2>, <c,1>\}$ is a function, but $f^{-1}=\{<1,a>, <2,b>, <1,c>\}$ is not a function.

- $f: A \rightarrow B$ is called an invertible function, if its inverse relation, $f^{-1}: B \rightarrow A$ is also a function.
  - Example: $f: N \times N \rightarrow N$, $f(<i,j>)=2^i(2j+1)-1$ is a bijection

    $f^{-1}(2^i(2j+1)-1)=<i,j>$

Invertible Function

- $f : A \to B$ has an invertible function if and only if f is a one-to-one.
  - Sketch of proof:

  $\Rightarrow$ If f is **not** a injection, there must be $<y,x_1>, <y,x_2> \in f^{-1}$, and $x_1 \neq x_2$, i.e. f is not a function, i.e. f is not invertible.

  $\Leftarrow$ If f^{-1} is **not** a function, then, either there exist $<y,x_1>$, $<y,x_2> \in f^{-1}$, and $x_1 \neq x_2$, then f is not a injection

  Contradition!

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 verse vica.
  - To prove $A \approx B$， find a one-to-one correspondence from A to B, any one.
- Two equipotent sets can be think as with “the same size.”

(Infinite) Countable Set

- A finite set is countable if it is equipotent to the set of natural number.
  - 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.

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

Finite Set and Infinite Set

- A set S is finite， iff. S is equipotent to some natural number n.
- A set S is infinite, iff. existing a proper subset of S, say S', S ≈ S'.

$\Rightarrow$ S must have a subset, M = $\{a_1,a_2,a_3,\ldots\}$, equipotent to the set of natural set (which means that the set of natural number is one of the "smallest" infinite set)

Let $S'=S-\{a_1\}$， define f:S→S' as follows:

for any $x\in M$, $f(a_i)= a_{i+1}$;   and for any $x\in S-M$, $f(x)= x$

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

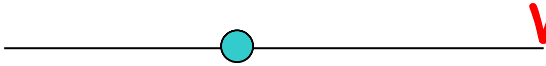
- (0,1) is equipotent to the set of all real number:
  - One-to-one correspondence： $f:(0,1)\rightarrow \boldsymbol{R}: f(x) = \mathrm{tg}(\pi x - \frac{\pi}{2})$
- For any two real numbers a,b($a<b$), [0,1] and [a,b] are equipotent:
  - One-to-one correspondence： $f:[0,1]\rightarrow[a,b]: f(x) = (b-a)x+a$

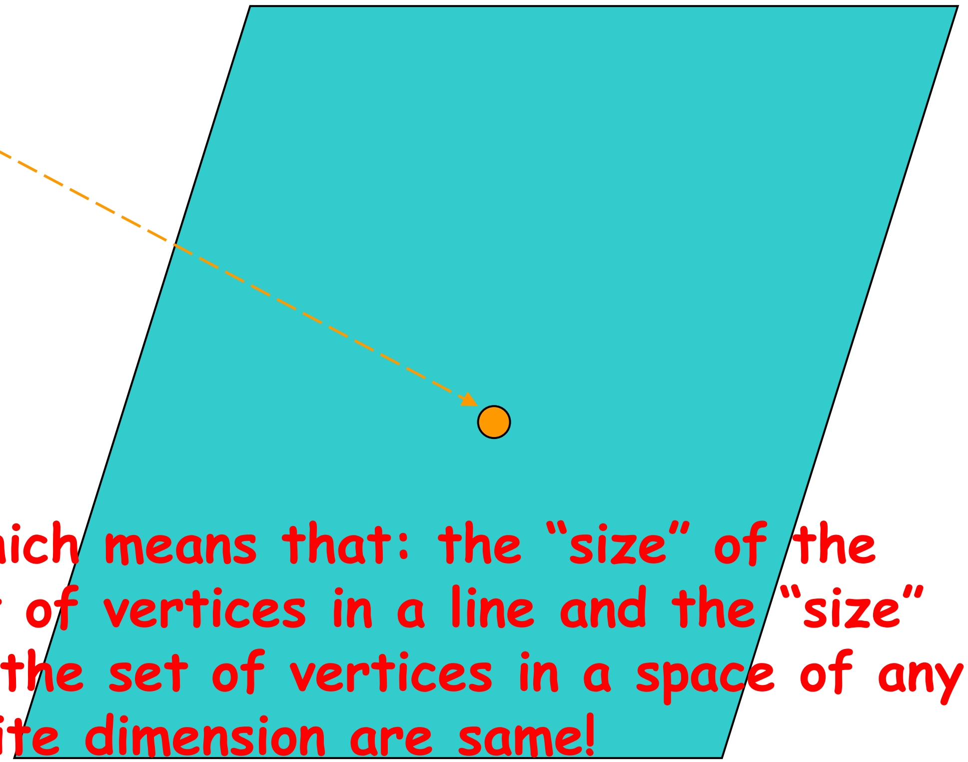
(In fact, any two line segments with different length are equipotent.)

Line and Plane

$$\left\{\begin{array}{l} 0.a_1a_2a_3....... \\ 0.b_1b_2b_3...... \end{array}\right.$$

$$0.a_1b_1a_2b_2a_3b_3.....$$





Which means that: the "size" of the set of vertices in a line and the "size" of the set of vertices in a space of any finite dimension are same!

Cantor's Theorem

- A set *S* cannot be equipotent to its power set, that is, $A \not\approx \rho(A)$
- Sketch of the proof

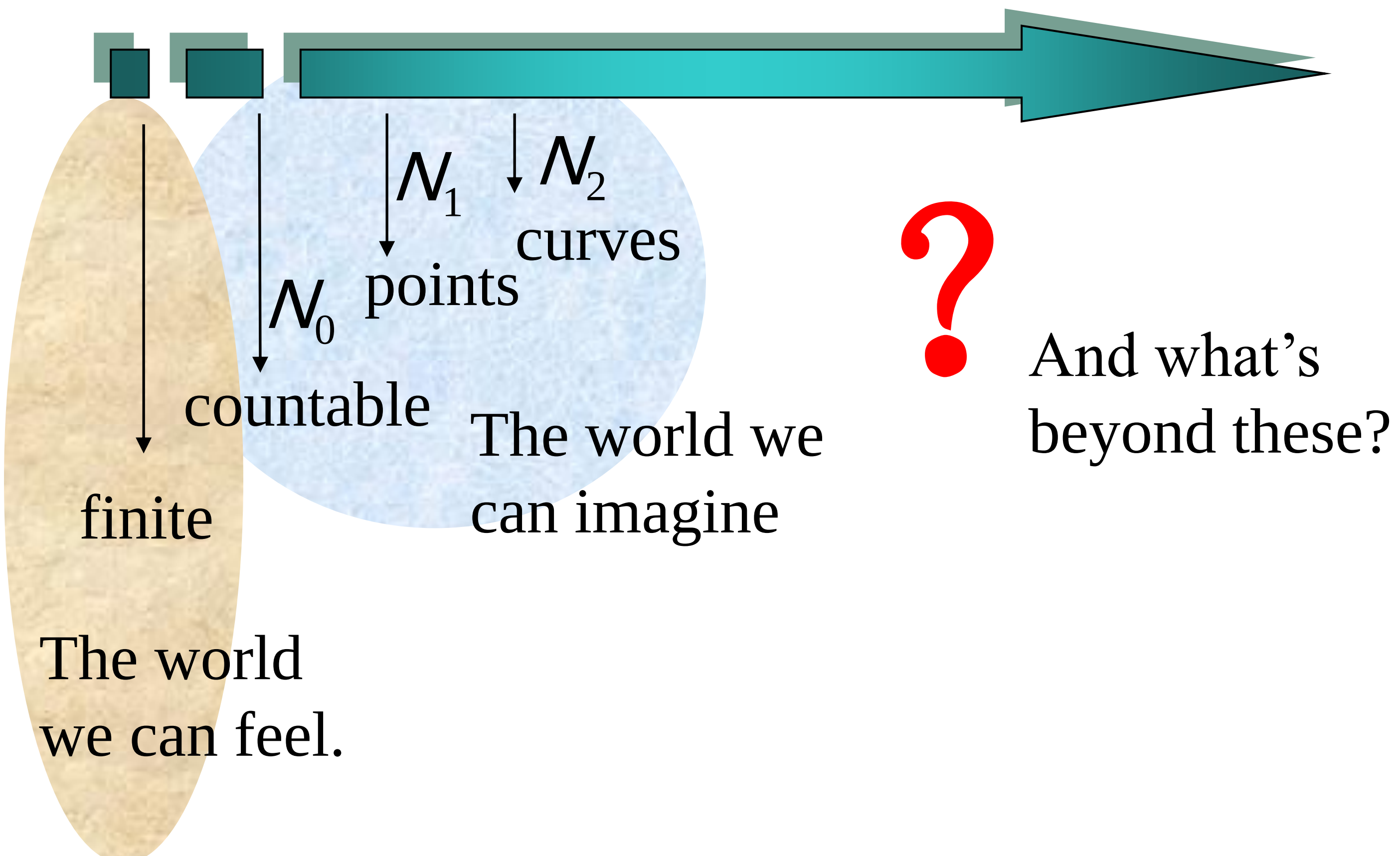
  Let g be a function from A to $\rho(A)$, define a set B as follows:

  $B=\{x \mid x \in A, \text{ and } x \notin g(x)\}$

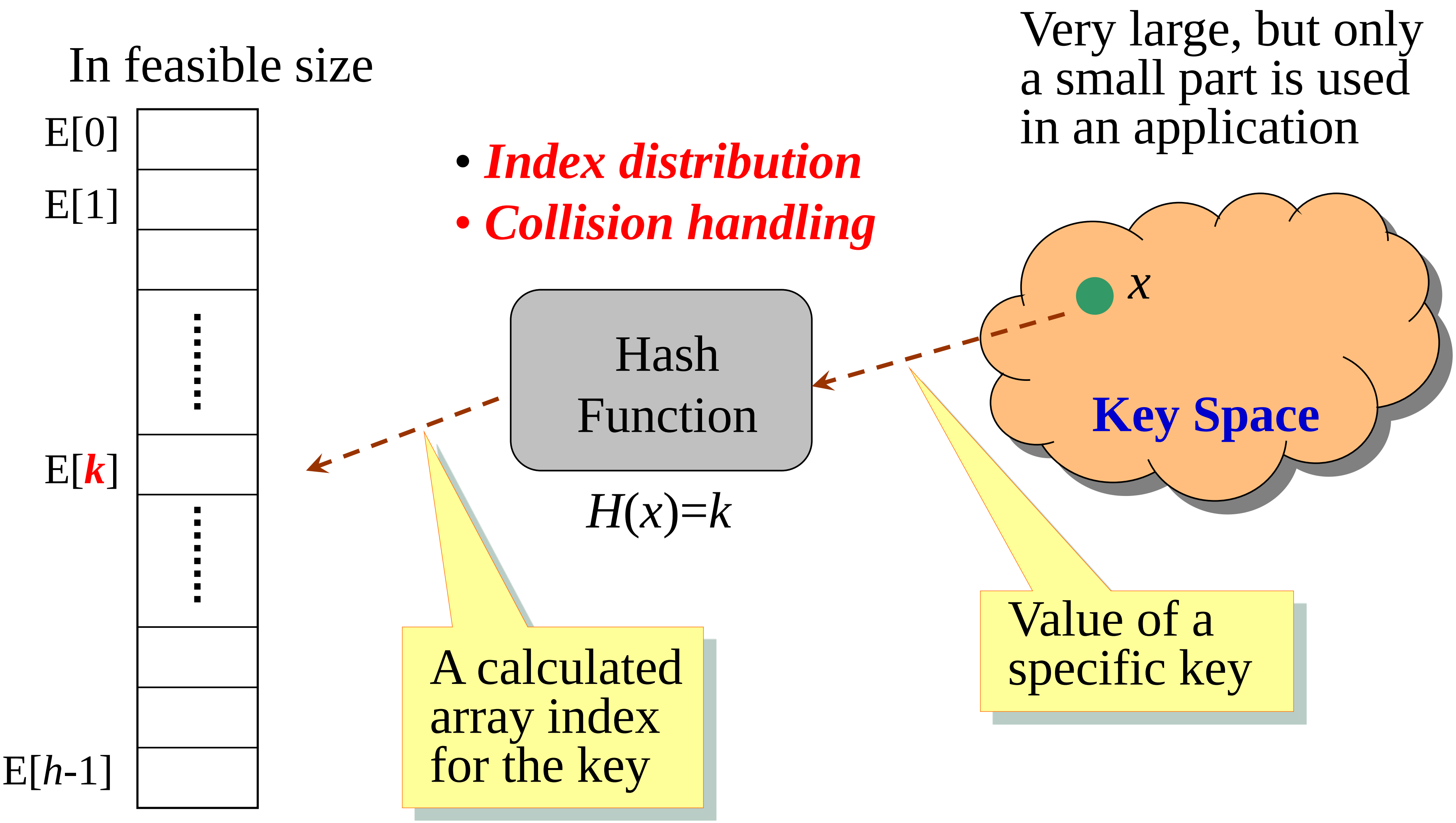
  So, $B \in \rho(A)$, but it is impossible that for some $x \in A$, such that $g(x)=B$, otherwise, $x \in B$ iff. $x \notin B$.

  So, g cannot be surjection, nor one-to-one correspondence, of course.

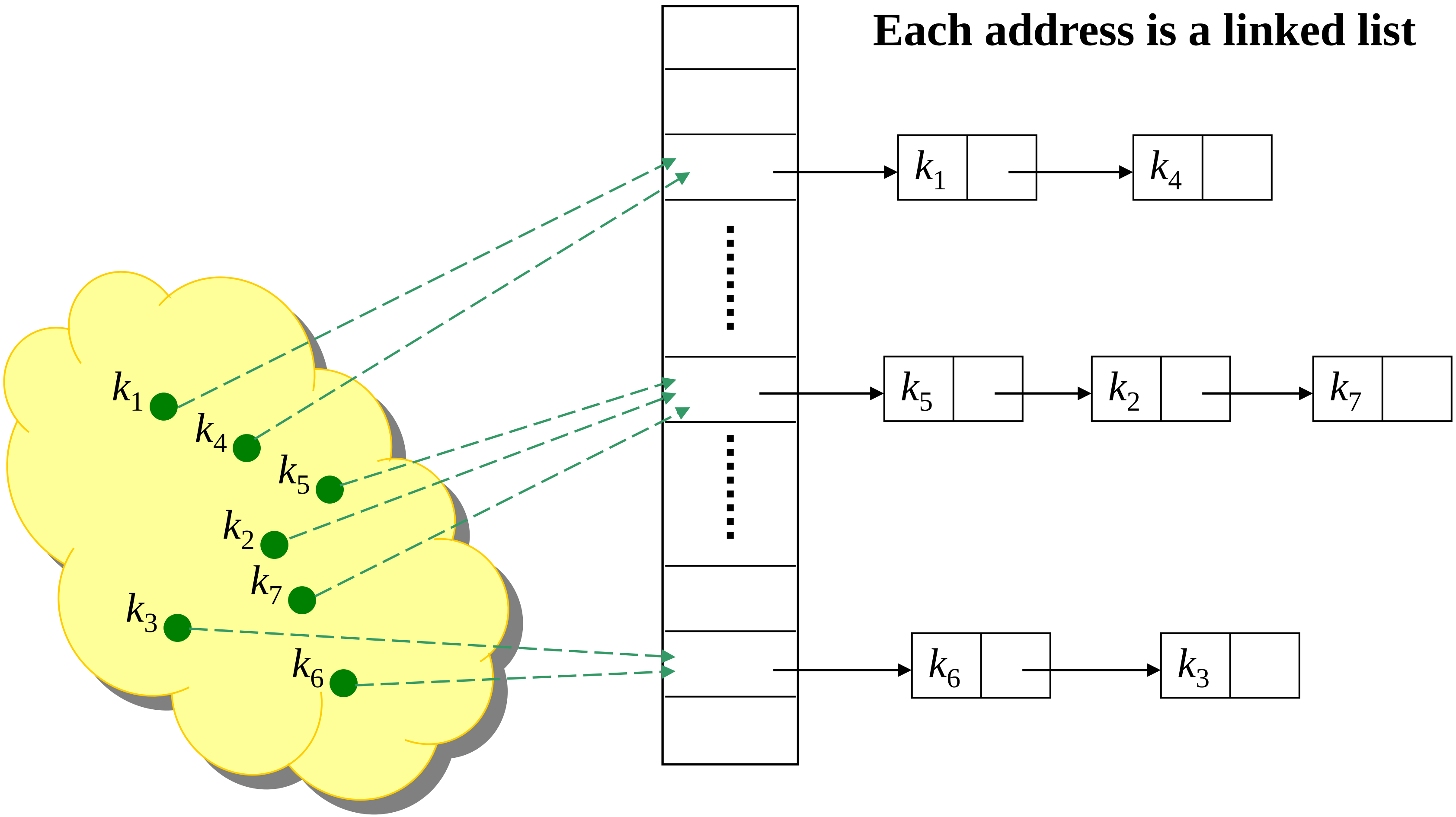
Size of Set – Cardinality



Hashing: the Idea



Collision Handling: Closed Address



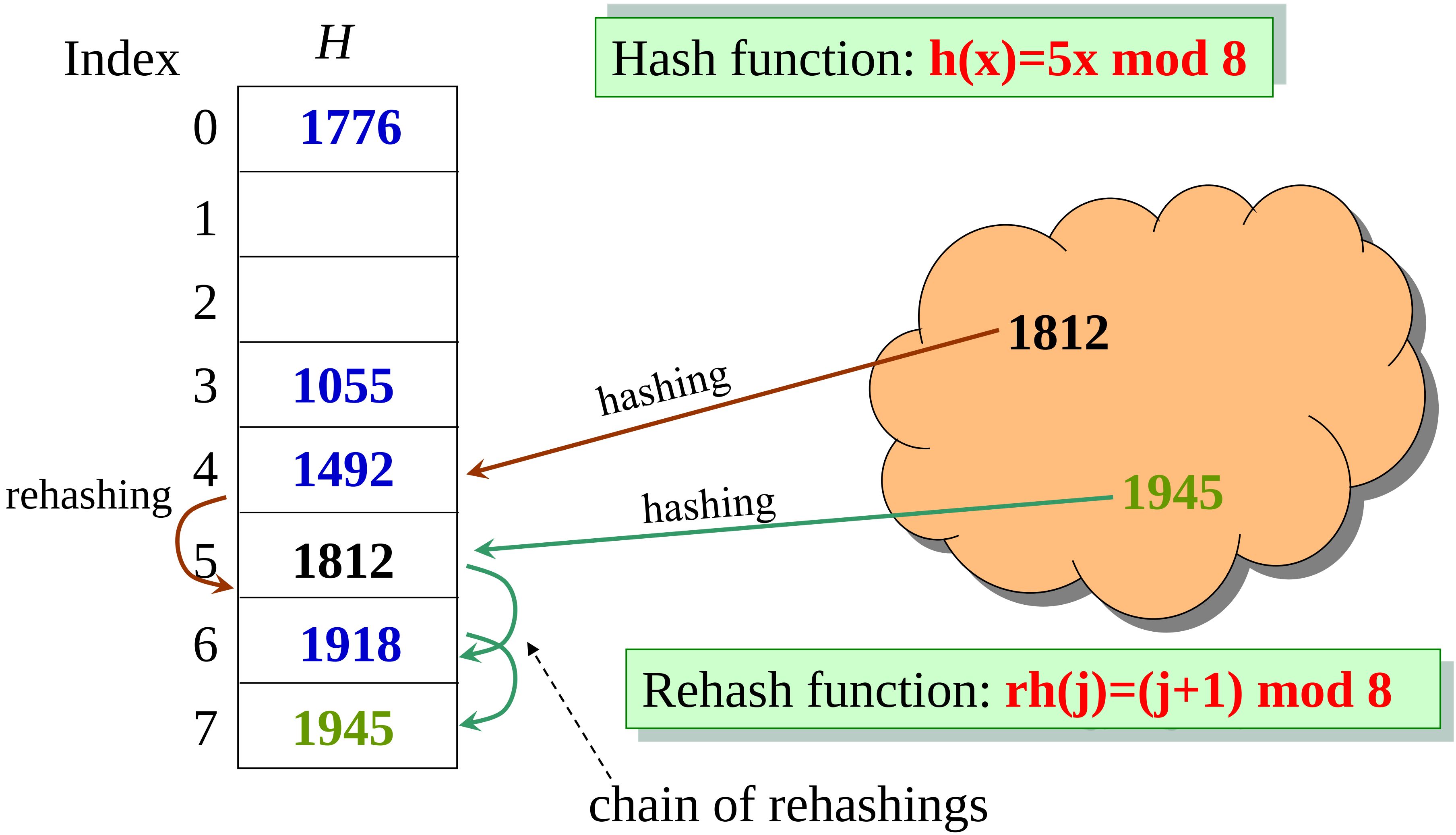
Collision Handling: Open Address

- 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 $(0,1,2,\ldots, h\text{-}1)$

Linear Probing: an Example



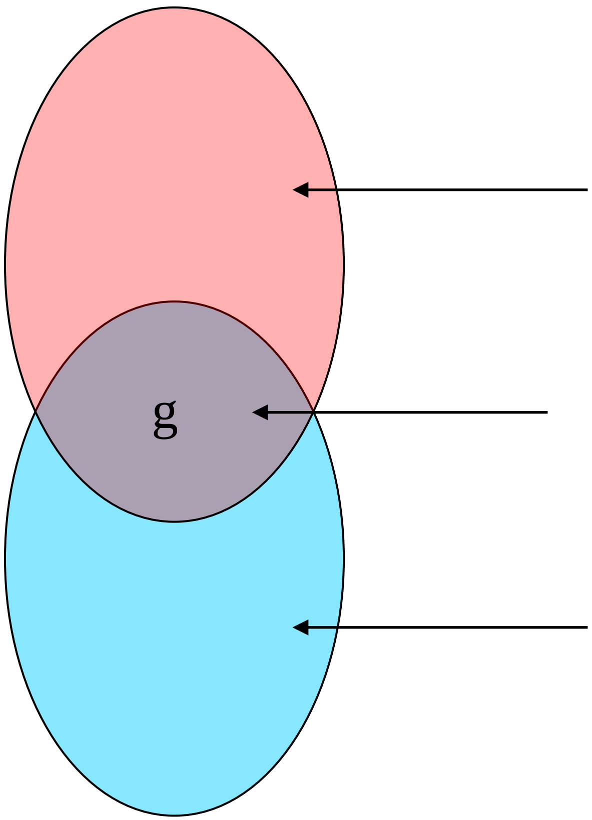
Hashing Function

- A good hash function satisfies the assumption of simple uniform hashing.
- Heuristic hashing functions
  - The divesion 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



Ω (g):functions that grow at least as fast as g

Θ (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:N→R$^+$, then O(g) is the set of f:N→R$^+$, such that for some c∈R$^+$ and some n_0∈N, f(n)≤cg(n) for all n≥n_0.
- A function f∈O(g) if $\lim_{n\to\infty}[f(n)/g(n)]=c<\infty$
  - Note: c may be zero. In that case, f∈o(g), "little Oh"
- Example: let $f(n)=n^2$, $g(n)=n\lg n$, then:
  - $f\notin O(g)$, since $\lim_{n\to\infty}[f(n)/g(n)]= \lim_{n\to\infty}[n^2/n\lg n]= \lim_{n\to\infty}[n/\lg n]= \lim_{n\to\infty}[1/(1/n\ln 2)]=\infty$
  - $g\in O(f)$, since $\lim_{n\to\infty}[g(n)/f(n)]=0$

The Sets Ω and Θ

- Definition
  - Giving g:N→R$^+$, then $\Omega(g)$ is the set of f:N→R$^+$, such that for some c∈R$^+$ and some n_0∈N, $f(n) \geq cg(n)$ for all $n \geq n_0$.
- A function $f \in \Omega(g)$ if $\lim_{n\to\infty}[f(n)/g(n)]>0$
  - Note: the limit may be infinity
- Definition
  - Giving g:N→R$^+$, then $\Theta(g) = O(g) \cap \Omega(g)$
- A function $f \in O(g)$ if $\lim_{n\to\infty}[f(n)/g(n)]=c, 0<c<\infty$

How Functions Grow

Algorithm	1	2	3	4	
Time function(ms)	$33n$	$46n \lg n$	$13n^2$	$3.4n^3$	2^n
Input size(n)			Solution time		
10	0.00033 sec.	0.0015 sec.	0.0013 sec.	0.0034 sec.	0.001 sec.
100	0.0033 sec.	0.03 sec.	0.13 sec.	3.4 sec.	4×10^{16} yr.
1,000	0.033 sec.	0.45 sec.	13 sec.	0.94 hr.	
10,000	0.33 sec.	6.1 sec.	22 min.	39 days	
100,000	3.3 sec.	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	$t\ s_2$
n^2	s_3	$\sqrt{t}\ s_3$
n^3	s_4	$s_4\text{+lg } n$

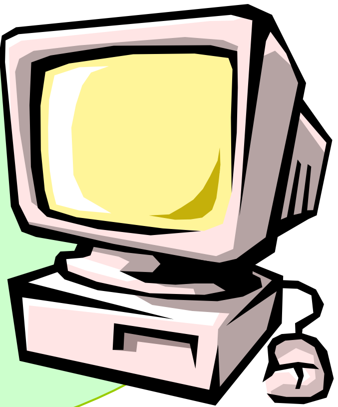
Sorting a Array of 1 Million Numbers

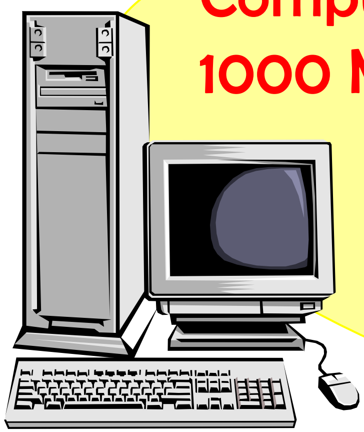
Using ***merge sort***, taking time $50n\log n$:

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:N→R* under consideration, define the relation ~ on S as following: $f \sim g$ iff. $f \in \Theta(g)$

  then, ~ 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

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

(The commonly seen base is 2)

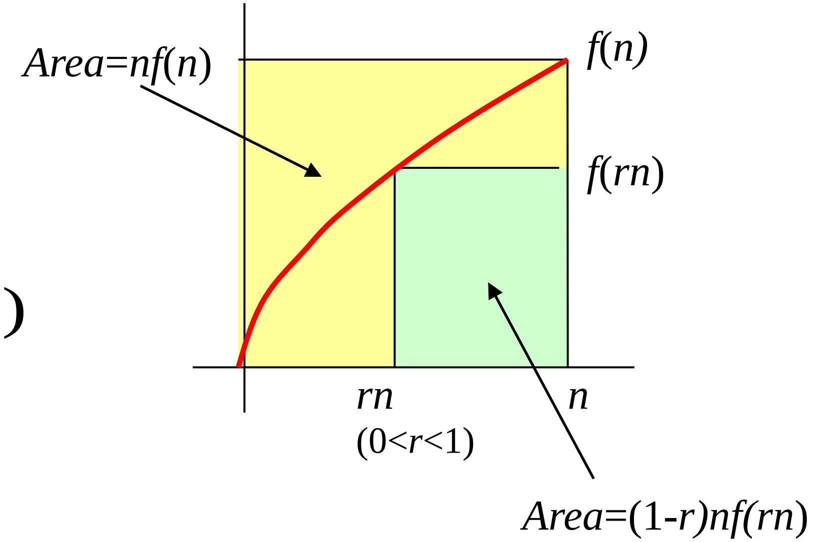
Order of Common Sums

$$\sum_{i=1}^{n} i^{d} \in \Theta\left(n^{d+1}\right)$$

$$\sum_{i=a}^{b} r^{i} \in \Theta(r^{k})$$ r^k is the largest term in the sum

$$\sum_{i=1}^{n} \log(i) \in \Theta(n \log n)$$

$$\sum_{i=1}^{n} i^{d} \log(i) \in \Theta(n^{d+1} \log(n))$$



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 of Permutation

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

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

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

Cyclic Permutation and Transposition

- If p is a permutation of S={1,2,…,n}, and
  $p(i_1)=i_2$, $p(i_2)=i_3$, …, $p(i_{k-1})=i_k$, $p(i_k)=i_1$,
  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: $(i_1\ i_2\ \ldots\ i_k)$
- 6 permutation of S={1,2,3}:
  - e=(1); α=(1 2 3); β=(1 3 2); γ=(2 3); δ=(1 3); ε=(1 2)

Disjoint Cyclic Permutations

- Given two cyclic permutations of S:

  $p = (i_1\ i_2\ \ldots\ i_k),\ q = (j_1\ j_2\ \ldots\ j_s)$,

  if $\{i_1, i_2, \ldots, i_k\} \cap \{j_1, j_2, \ldots, j_s\} = \phi$, 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:
  - $x \in \{i_1, i_2, \ldots, i_k\}$;
  - $x \in \{j_1, j_2, \ldots, j_s\}$;
  - $x \in S - (\{i_1, i_2, \ldots, i_k\} \cup \{j_1, j_2, \ldots, j_s\})$,

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

Permutation as Product of Cycles

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

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

Permutation as Product of Transpositions

- Every cycle $p=(i_1\ i_2\ \dots\ i_k)$ can be represented as a product of k-1 transpositions $(i_1 i_k)(i_1 i_{k-1}),\dots,(i_1 i_2)$
  - The order cannot be changed.

- Proof by induction on k:
  - k=2 is trivial.
  - Considering $p=(i_1\ i_2\ \dots\ i_k\ i_{k+1})$, to prove that $p=(\mathrm{i}_1\ \mathrm{i}_{k+1})(\mathrm{i}_1\ \mathrm{i}_2\ \dots\ \mathrm{i}_k)$

    i.e， for any $x\in$ A, $p(x)=(i_1\ i_{k+1})(i_1\ i_2\ \dots\ i_k)\ (x)$

    (1) $x\in\{ i_1, i_2, \dots, i_{k-1}\}$

    (2) $x=i_k$

    (3) $x=i_{k+1}$

    (4) otherwise

Permutation as Product of Cycles

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

  $= \mathbf{(1\ 7)\ (1\ 5)\ (4\ 8)}$

  Odd

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

  $= \mathbf{(1\ 5)\ (1\ 3)\ (1\ 2)\ (4\ 6)\ (4\ 7)\ (4\ 8)}$

  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