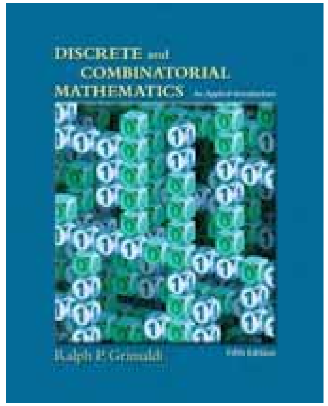
Discrete Mathematics

-- Chapter 5: Relations and Functions



Hung-Yu Kao (高宏宇)
Department of Computer Science and Information Engineering,
National Cheng Kung University

Outline

- 5.1 Cartesian Products and Relations
- 5.2 Functions: Plain and One-to-One
- 5.3 Onto Functions: Stirling Numbers of the Second Kind
- 5.4 Special Functions

- 5.6 Function Composition and Inverse Functions

- 5.7 Computational Complexity
- 5.8 Analysis of Algorithms

5.1 Cartesian Products and Relations

- For sets A, B, the Cartesian product (cross product), of A and B is denoted by $A \times B = \{(a,b) \mid a \in A, b \in B\}$.
  - E.g., {a,b} × {1,2,3} = {(a,1),(b,1),(a,2),(b,2),(a,3),(b,3)}
- Extension of the Cartesian product:
  $A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in A_i, 1 \le i \le n\}$.

- **Ex 5.2** : $\mathbf{R} \times \mathbf{R} = \{(x, y) \mid x, y \in \mathbf{R}\}$ is recognized as the real plane of coordinate geometry and two-dimensional calculus.
  - The subset $\mathbf{R}^+ \times \mathbf{R}^+$ is the interior of the first quadrant of this plane.
  - $\mathbf{R}^3$ represents Euclidean three-space, where the three-dimensional interior of any sphere, and two-dimensional planes, and one-dimensional lines are subsets of importance.

Cartesian Products and Relations

- **Ex 5.1** : Let A = {2, 3, 4}, B = {4, 5}. Then

a) $A \times B = \{(2,4),(2,5),(3,4),(3,5),(4,4),(4,5)\}$

b) $B \times A = \{(4,2),(4,3),(4,4),(5,2),(5,3),(5,4)\}$

c) $B^2 = B \times B = \{(4,4),(4,5),(5,4),(5,5)\}$

d) $B^3 = B \times B \times B = \{(a,b,c) \mid a,b,c \in B\}$; e.g., $(4,5,5) \in B^3$

- **Ex 5.3:** Tree diagram
  - C = {x, y}
  - |A x B x C| = 12
    = 3 * 2 * 2 = |A||B||C|

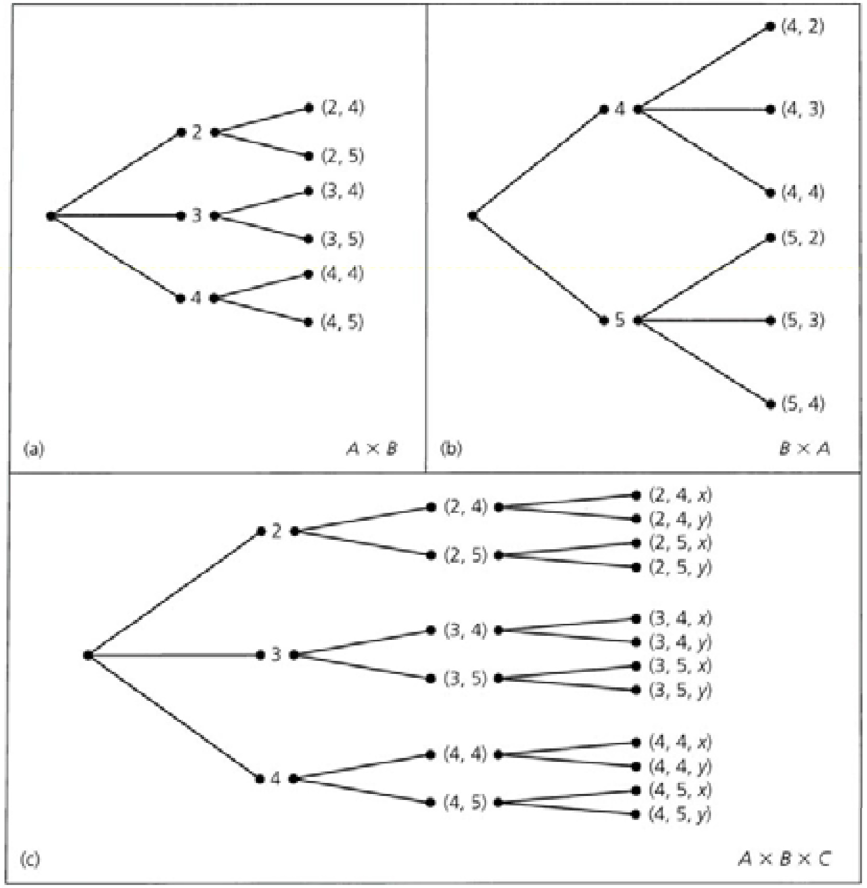


Figure 5.1

Cartesian Products and Relations

- Definition 5.2: For sets A, B, any subset of $A \times B$ is called a (binary) relation from A to B. Any subset of $A \times A$ is called a (binary) relation on A.
- In short, we say "aRb" if and only if $(a,b) \in R$.

- **Ex 5.5** : The following are some of the relations from A to B.
  - $\phi, \{(2,4),(3,5)\}, A \times B$
  - $\because |A \times B| = 6, \therefore 2^6$ possible relations from A to B
  - General formula : $|A| = m, |B| = n, 2^{mn}$ relations from A to B

- How many relations from B to A?

Cartesian Products and Relations

- **Ex 5.7** : $A = \mathbf{Z}^+$, we may define a relation $\Re$ on set A as $\{(x, y) \mid x \le y\}$
  $\Re$ is the relation "is less than or equal to".
  $(7,7), (7,11) \in \Re$, or $7 \Re 7$, $7 \Re 11$
  $(8,2) \notin \Re$, or $8 \not\Re 2$

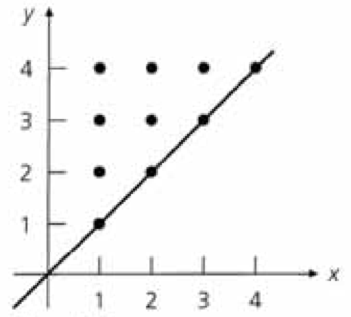


Figure 5.3

- For any set A, $A \times \phi = \phi, \phi \times A = \phi$

Cartesian Products and Relations

- Theorem 5.1: For any sets $A, B, C \subseteq$ h :

$$\text{a) } A \times (B \cap \mathrm{C}) = (A \times B) \cap (A \times \mathrm{C})$$

$$\text{b) } A \times (B \cup \mathrm{C}) = (A \times B) \cup (A \times \mathrm{C})$$

$$\text{c) } (A \cap B) \times \mathrm{C} = (A \times \mathrm{C}) \cap (B \times C)$$

$$\text{d) } (A \cup B) \times \mathrm{C} = (A \times \mathrm{C}) \cup (B \times \mathrm{C})$$

- Proof

$$\text{(a) } \forall a, b \in A \times (B \cap \mathrm{C}) \Leftrightarrow a \in A \text{ and } b \in (B \cap \mathrm{C})$$

$$\Leftrightarrow a \in A \text{ and } b \in B \cap b \in \mathrm{C} \Leftrightarrow a \in A\,, b \in B \text{ and } a \in A, b \in \mathrm{C}$$

$$\Leftrightarrow (a, b) \in A \times B \text{ and} (a, b) \in A \times \mathrm{C}$$

$$\Leftrightarrow (a, b) \in (A \times B) \cap (A \times \mathrm{C})$$

5.2: Functions: Plain and One-to-One

- Definition 5.3: for nonempty sets A, B, $f: A \to B$, a function (mapping) from A to B, is a relation from A to B in which every element of A appears exactly once as the first component of an ordered pair in the relation.
  - $f(a) = b$ when (a, b) is an ordered pair in the function f.
  - $(a, b) \in f$, b is called the image of a under f, whereas a is a preimage of b.
  - f is a method for associating with each $a \in A$ the **unique** element $f(a) = b \in B$.
  - $(a, b), (a, c) \in f$, implies $b = c$.
- **Ex 5.9** :

$$A = \{1,2,3\}, B = \{w, x, y, z\}$$
$$f = \{(1, w), (2, x), (3, x)\} \text{ is a function and a relation}$$
$$\Re_1 = \{(1, w), (2, x)\}, \Re_2 = \{(1, w), (2, w), (2, x), (3, z)\} \text{ are relations, but not functions.}$$

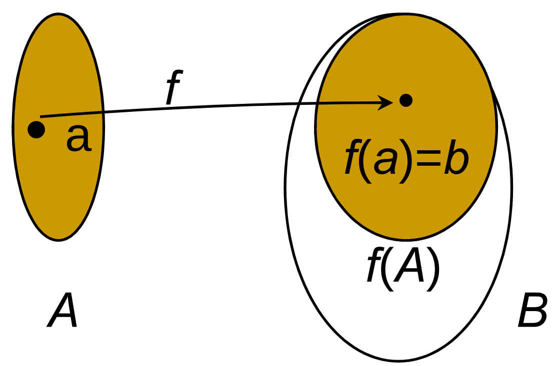
Functions: Plain and One-to-One

- Definition 5.4: Function $f : A \to B$, A is called the <u>domain</u> of f and B the <u>codomain</u> of f.
  - The subset of B consisting of those elements that appear as second components in the ordered pairs of f is called the <u>range</u> of f and is also denoted by $f(A)$ because it is the set of images (of the elements of A) under f.
  - In Example 5.9,

    the domain of $f = \{1,2,3\}$

    the codomain of $f = \{w, x, y, z\}$

    the range of $f = f(A) = \{w, x\}$



- A C++ compiler can be thought of as a function that transforms a source program (the input) into its corresponding object program (the output).

Functions: Plain and One-to-One

- **Ex 5.10** Many interesting function arise in computer science.
  - (a) Greatest integer function (floor function)

    $f : \mathbf{R} \to \mathbf{Z}, f(x) = \lfloor x \rfloor =$ the greatest integer less than or equal to x.

    1) $\lfloor 3.8 \rfloor = 3, \lfloor 3 \rfloor = 3, \lfloor -3.8 \rfloor = -4, \lfloor -3 \rfloor = -3$

    2) $\lfloor 7.1 + 8.2 \rfloor = \lfloor 15.3 \rfloor = 15 = 7 + 8 = \lfloor 7.1 \rfloor + \lfloor 8.2 \rfloor$

    3) $\lfloor 7.7 + 8.4 \rfloor = \lfloor 16.1 \rfloor = 16 \neq 15 = 7 + 8 = \lfloor 7.7 \rfloor + \lfloor 8.4 \rfloor$
  - (b) Ceiling function

    $g : \mathbf{R} \to \mathbf{Z}, g(x) = \lceil x \rceil =$ the least integer greater than or equal to x.

    1) $\lceil 3 \rceil = 3, \lceil 3.01 \rceil = \lceil 3.7 \rceil = 4 = \lceil 4 \rceil, \lceil -3 \rceil = -3, \lceil -3.01 \rceil = \lceil -3.7 \rceil = -3$

    2) $\lceil 3.6 + 4.5 \rceil = \lceil 8.1 \rceil = 9 = 4 + 5 = \lceil 3.6 \rceil + \lceil 4.5 \rceil$

    3) $\lceil 3.3 + 4.2 \rceil = \lceil 7.5 \rceil = 8 \neq 9 = 4 + 5 = \lceil 3.3 \rceil + \lceil 4.2 \rceil$
  - (c) Truncation (trunc) function: delete the fractional part of a real number
    - trunc(3.78) = 3, trunc(5) = 5, trunc(-7.22) = -7
    - $\text{trunc}(3.78) = \lfloor 3.78 \rfloor = 3, \text{trunc}(-3.78) = \lceil -3.78 \rceil = -3$

Functions: Plain and One-to-One

- (d) Access function: storing a $m \times n$ matrix in a one-dimensional array
  - Use the row major implementation
  - formula : $f(a_{ij}) = (i-1)n + j$

a_{11}	a_{12}	…	a_{1n}	a_{21}	a_{22}	…	a_{2n}	a_{31}	…	a_{ij}	…	a_{mn}
1	2	…	n	n+1	n+2	…	2n	2n+1	…	(i-1)n+j	…	(m-1)n+n=mn

Functions: Plain and One-to-One

- **Ex 5.12**
  - A sequence of real numbers $r_1, r_2, r_3, \ldots$ can be thought of as a function $f: \mathbf{Z}^+ \to \mathbf{R}$ where $f(n) = r_n$, for all $n \in \mathbf{Z}^+$.
  - An integer sequence $a_0, a_1, a_2, \ldots$ can be defined by means of a function $g: \mathbf{N} \to \mathbf{Z}$ where $g(n) = a_n$, for all $n \in \mathbf{N}$.

- Let A, B be nonempty sets with $|A| = m$, $|B| = n$, $A = \{a_1, a_2, \ldots, a_m\}$ and $B = \{b_1, b_2, \ldots, b_n\}$, a typical function $f: A \to B$ can be described by $\{(a_1, x_1), (a_2, x_2), \ldots, (a_m x_m)\}$. We can select any of n elements of B for x_1 and do the same for x_2, continuing until x_m. So, there are $n^m = |B|^{|A|}$ functions from A to B.
  - E.g., In Example 5.9, $|A| = 3$, $|B| = 4$, there are 4^3 functions from A to B, and 3^4=81 functions from B to A.

Functions: Plain and One-to-One

- Definition 5.5: A function $f : A \to B$ is called <u>one-to-one</u> (<u>injective</u>), if each element of B appears at most once as the image of an element of A.
  - If $f : A \to B$ is one-to-one, with A, B finite, we must have $|A| \leq |B|$.
  - $f : A \to B$ is one-to-one if and only if for all $a_1, a_2 \in A, f(a_1) = f(a_2) \Rightarrow a_1 = a_2$
- **<u>Ex 5.13</u>** :

  Consider the function $f : \mathbf{R} \to \mathbf{R}$ where $f(x) = 3x + 7$, for all $x \in \mathbf{R}$

  Then for all $x_1, x_2 \in \mathbf{R}$

  $f(x_1) = f(x_2) \Rightarrow 3x_1 + 7 = 3x_2 + 7 \Rightarrow 3x_1 = 3x_2 \Rightarrow x_1 = x_2$

  so f is one-to-one.

Functions: Plain and One-to-One

- **Ex 5.13**
  - Suppose that $g : \mathbf{R} \to \mathbf{R}$ where $g(x) = x^4 - x$, for all $x \in \mathbf{R}$

    $g(0) = 0^4 - 0 = 0$ and $g(1) = 1^4 - 1 = 0$

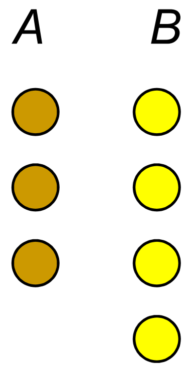
    so g is not one-to-one ($\because g(0) = g(1)$ but $0 \neq 1$)
- **Ex 5.14**
  - $A = \{1,2,3\}, B = \{1,2,3,4,5\}$

    $f = \{(1,1),(2,3),(3,4)\}$ is a one-to-one function from A to B

    $g = \{(1,1),(2,3),(3,3)\}$ is a function from A to B, but is not one-to-one

    ($\because g(2) = g(3)$ but $2 \neq 3$)
  - 2^{15} relations from A to B, 5^3 functions
  - how many functions are one-to-one? 5*4*3=60

Functions: Plain and One-to-One



- $A=\{a_1,a_2,\ldots,a_m\}, B=\{b_1,b_2,\ldots,b_n\}$, and $m \le n$, there are

  a) 2^{mn} realtions from A to B

  b) n^m functions from A to B

  c) $P(|B|,|A|)=P(n,m)=n(n-1)(n-2)\cdots(n-m+1)$ one - to - one functions from A to B

- Definition 5.6:

  If $f: A \to B$ and $A_1 \subseteq A$, then $f(A_1)=\{b \in B \mid b=f(a), \text{ for some } a \in A_1\}$ and $f(A_1)$ is called the <u>image</u> of A_1 under f.

Functions: Plain and One-to-One

- **Ex 5.15** :

  $A=\{1,2,3,4,5\}, B=\{w,x,y,z\}, f=\{(1,w),(2,x),(3,x),(4,y),(5,y)\}$

  $A_1=\{1\}, A_2=\{1,2\}, A_3=\{1,2,3\}, A_4=\{2,3\}, A_5=\{2,3,4,5\}$

  Corresponding images under f

  $f(A_1)=\{f(a)\mid a\in A_1\}=\{f(a)\mid a\in\{1\}\}=\{f(1)\}=\{w\}$

  $f(A_2)=\{f(a)\mid a\in A_2\}=\{f(a)\mid a\in\{1,2\}\}=\{f(1),f(2)\}=\{w,x\}$

  $f(A_3)=\{f(a)\mid a\in A_3\}=\{f(a)\mid a\in\{1,2,3\}\}=\{f(1),f(2),f(3)\}=\{w,x\}$

  $f(A_4)=\{x\}$ and $f(A_5)=\{x,y\}$

- **Ex 5.16** :

  (a) If $g:\mathbf{R}\to\mathbf{R}$ and $g(x)=x^2$, then $g(\mathbf{R})=$ the range of $g=[0,+\infty)$.

  The image of $\mathbf{Z}$ under g is $g(Z)=\{0,1,4,9,16,\cdots\}$, and $A_1=[-2,1]\Rightarrow g(A_1)=[0,4]$.

  (b) $h:\mathbf{Z}\times\mathbf{Z}\to\mathbf{Z}$ and $h(x,y)=2x+3y$, the domain of h is $\mathbf{Z}\times\mathbf{Z}$, the codomain is $\mathbf{Z}$

  for $A_1=\{(0,n)\mid n\in\mathbf{Z}^+\}=\{0\}\times\mathbf{Z}^+\subseteq\mathbf{Z}\times\mathbf{Z}$, the image of A_1 under h is $h(A_1)=\{3n\mid n\in\mathbf{Z}^+\}$

Functions: Plain and One-to-One

- Theorem 5.2: Let $f: A \to B$, with $A_1, A_2 \subseteq A$. Then
  (a) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$
  (b) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$
  (c) $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ when f is one-to-one.

Pick up $A_1 \cap A_2 = \phi$

- Definition 5.7: Let $f: A \to B$, and $A_1 \subseteq A$, then $f|_{A_1}: A_1 \to B$ is called the restriction of f to A_1 if $f|_{A_1}(a) = f(a)$ for all $a \in A_1$.
- Definition 5.8: Let $A_1 \subseteq A$ and $f: A_1 \to B$. If $g: A \to B$ and $g(a) = f(a)$ for all $a \in A_1$, then we call g an extension of f to A.

Functions: Plain and One-to-One

- **Ex 5.18** : Let $A=\{w,x,y,z\}$, $B=\{1,2,3,4,5\}$, $A_1=\{w,y,z\}$
  $f:A\to B, g:A_1\to B$
  $g=f|_{A_1}$ and f is an extension of g from A_1 to A.
  There are 5 ways to extend g from A_1 to A.

=>

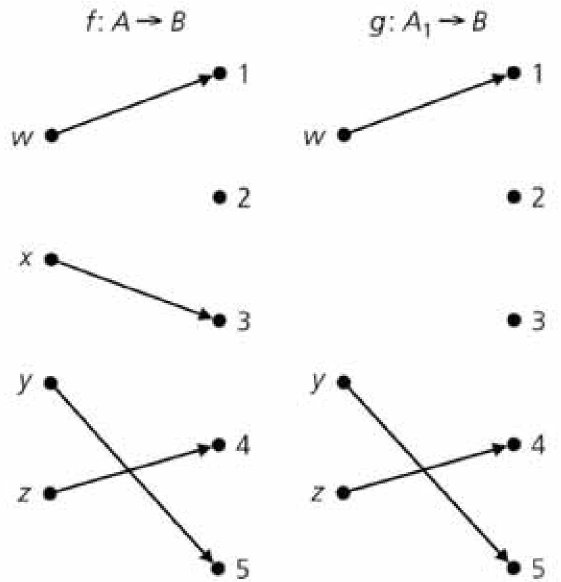


Figure 5.5

5.3 Onto Functions: Stirling Numbers of the Second Kind

- Definition 5.9: A function $f: A \to B$ is called **onto** (**surjective**) if $f(A) = B$, i.e., for all $b \in B$ there is **at least one** $a \in A$ with $f(a) = b$.
- **Ex 5.19** :

$$f: \mathbf{R} \to \mathbf{R} \text{ with } f(x) = x^3 \text{ is an onto function.}$$

$$g: \mathbf{R} \to \mathbf{R} \text{ with } g(x) = x^2 \text{ is not onto.}$$

$$h: \mathbf{R} \to [0, +\infty) \text{ with } h(x) = x^2 \text{ is an onto function.}$$

- **Ex 5.20** :

$$f: \mathbf{Z} \to \mathbf{Z} \text{ with } f(x) = 3x + 1 \text{ is not onto.}$$

$$g: \mathbf{Q} \to \mathbf{Q} \text{ with } g(x) = 3x + 1 \text{ is an onto function .}$$

$$h: \mathbf{R} \to \mathbf{R} \text{ with } h(x) = 3x + 1 \text{ is an onto function.}$$

Some Functions

The square function $f:Z \rightarrow N$, defined by $f(x)=x^2$.
$f(3)=9$, $f(0)=0$, $f^{-1}(4) = \{-2,+2\}$, $f^{-1}(3) = \emptyset$.
This f is not injective, nor surjective.

The square function $f:[0,2] \rightarrow [-4,4]$ is injective, but not surjective ($f^{-1}(-2) = \emptyset$)

The linear function $f:Z \rightarrow Z$, defined by $f(x)=x+2$.
$f(3)=5$, $f(0)=2$, $f^{-1}(4) = 2$.
This f is injective and surjective: it is a bijection.

The identity $I:A \rightarrow A$ is always a bijection.

Counting with Functions

- If $f:A \rightarrow B$ is injective then $|B| \geq |A|$.
- If $f:A \rightarrow B$ is surjective then $|A| \geq |B|$.
- If $f:A \rightarrow B$ is bijective then $|A| = |B|$.
- This still makes sense for infinite sized sets…

How Many Functions?

For the finite sets $A = \{a_1,\ldots,a_m\}$ and $B = \{b_1,\ldots,b_n\}$, how many functions $f:A\rightarrow B$ are there?

Total number of all functions (trivial): $|B|^{|A|} = n^m$.

One-to-one functions (easy): $|B|$ options for $f(a_1)$, $|B|-1$ options for $f(a_2),\ldots,$ $|B|-|A|+1$ options for $f(a_m)$.
By the product rule total there are in total
$n\cdot(n-1)\cdots(n-m+1) = n!/(n-m)! =$ **$P(n,m)$ injective functions**.

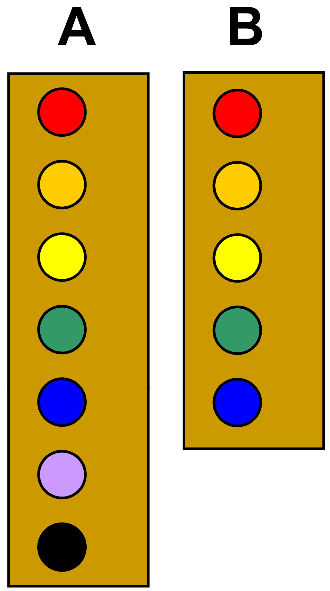
There are $P(m,m) =$ $m!$ bijections if $|A|=|B|=m$.

How Many Onto Functions?

- The question **how many onto (surjective) functions** there are from $A = \{a_1,\ldots,a_m\}$ and $B = \{b_1,\ldots,b_n\}$ is less easy.

- Observe:
  If $|A|<|B|$ then the number is 0.
  If $|A|=|B|$ then the number is m!

- For general $m \geq n$ …



Onto Functions: Stirling Numbers of the Second Kind

- **Ex 5.21** :
  If $A=\{1,2,3,4\}, B=\{x,y,z\}$,
  $f_1=\{(1,z),(2,y),(3,x),(4,y)\}, f_2=\{(1,x),(2,x),(3,y),(4,z)\}$
  are both functions from A onto B.
  $g=\{(1,x),(2,x),(3,y),(4,y)\}$ is not onto, $\because g(A)=\{x,y\}\neq B$.

- **Ex 5.22** :

  If $A=\{x,\mathrm{y},\mathrm{z}\}, B=\{1,2\}$, then all functions $f:A\rightarrow B$ are onto
  except $f_1=\{(x,1),(y,1),(z,1)\}, f_2=\{(x,2),(y,2),(z,2)\}$(the constant function)
  So there are $|B|^{|A|}-2=2^3-2=6$ onto functions from A to B.
  In general, if $|A|=m\geq 2$ and $|B|=2$ there are 2^m-2 onto functions from A to B.

  when m = 1?

5.3 Onto Functions: Stirling Numbers of the Second Kind

- **Ex 5.23** :

If $A=\{w,x,y,z\}, B=\{1,2,3\} \Rightarrow 3^4$ functions from A to B

Considering three subsets of B of size 2:

$$\Rightarrow \begin{cases} 2^4 \text{ functions from } A \text{ to } \{1,2\} \\ 2^4 \text{ functions from } A \text{ to } \{2,3\} \\ 2^4 \text{ functions from } A \text{ to } \{1,3\} \end{cases} \Rightarrow 3 \cdot 2^4 = \binom{3}{2} \cdot 2^4 \text{ functions from } A \text{ to } B \text{ that are not onto}$$

In fact, there are some functions are repeated twice, e.g.,

$$\begin{cases} \text{from } A \text{ to } \{1,2\} : \text{exists constant function } \{(w,2),(x,2),(y,2),(z,2)\} \\ \text{from } A \text{ to } \{2,3\} : \text{exists constant function } \{(w,2),(x,2),(y,2),(z,2)\} \end{cases}$$

$\Rightarrow 3 \cdot 1^4 = \binom{3}{1} \cdot 1^4$ functions are repeated from A to $\{1,2\}, \{2,3\}, \{1,3\}$

$\therefore$ there are some $\binom{3}{3} 3^4 - \binom{3}{2} 2^4 + \binom{3}{1} 1^4 = 36$ onto functions from A to B

If $|A| = m \geq 3, |B| = 3 \Rightarrow \binom{3}{3} 3^m - \binom{3}{2} 2^m + \binom{3}{1} 1^m$ onto functions from A to B

Onto Functions: Stirling Numbers of the Second Kind

- General formula: $|A| = m$, $|B| = n$, there are

$$\binom{n}{n}n^m - \binom{n}{n-1}(n-1)^m + \binom{n}{n-2}(n-2)^m - \cdots + (-1)^{n-2}\binom{n}{2}2^m + (-1)^{n-1}\binom{n}{1}1^m$$

$$= \sum_{k=0}^{n-1}(-1)^k\binom{n}{n-k}(n-k)^m = \sum_{k=0}^{n}(-1)^k\binom{n}{n-k}(n-k)^m$$

onto functions from A to B.

- Ex 5.24 :

Let $A = \{1,2,3,4,5,6,7\}$ and $B = \{w, x, y, z\}$

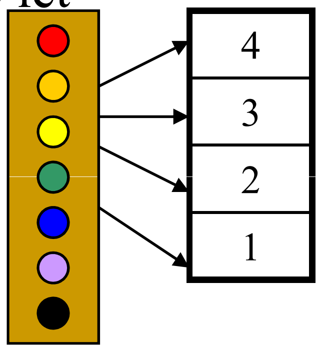
$$\binom{4}{4}4^7 - \binom{4}{3}3^7 + \binom{4}{2}2^7 - \binom{4}{1}1^7$$

$$= \sum_{k=0}^{3}(-1)^k\binom{4}{4-k}(4-k)^7 = \sum_{k=0}^{4}(-1)^k\binom{4}{4-k}(4-k)^7 = 8400$$

onto functions from A to B.

Onto Functions: Stirling Numbers of the Second Kind

- Problem 4: Seven (unrelated) people enter the lobby of a building which has four additional floors, and they all get on an elevator. What is the probability that the elevator must stop at every floor in order to let passengers off?
  - Solution



(i) sample space : $4^7 = 16{,}384$

the number is the same as the total number of functions

$f : A \to B$ where $|A| = 7, |B| = 4$

(ii) the number that the elevator must stop at every floor is also the answer of

the total number of onto functions $f : A \to B$ where $|A| = 7, |B| = 4$

$$\binom{4}{4}4^7 - \binom{4}{3}3^7 + \binom{4}{2}2^7 - \binom{4}{1}1^7 = 8400$$

$\therefore$ the probability $= \frac{8400}{16384} = 0.5127 > 0.5$

Onto Functions: Stirling Numbers of the Second Kind

- **Ex 5.25** : At the CH company, Joan, the supervisor, has a secretary, Teresa, and three other administrative assistants. If seven accounts must be processed, in how many ways can Joan assigns the accounts so that each assistant works on at least one account and Teresa's work includes **the most expensive account**?
  - Solution Consider two disjoint subcases:

    (i) Teresa woks only on the most expensive account

    the number of onto functions $f: A \to B$ where $|A| = 6, |B| = 3$

    $$\sum_{k=0}^{3} (-1)^k \binom{3}{3-k} (3-k)^6 = 540$$

    (ii) Teresa woks on more than just the most expensive account

    the number of onto functions $f: C \to D$ where $|C| = 6, |D| = 4$

    $$\sum_{k=0}^{4} (-1)^k \binom{4}{4-k} (4-k)^6 = 1560$$

    $\therefore 540 + 1560 = 2100$

    Difference with 8400?

Onto Functions: Stirling Numbers of the Second Kind

- **Ex 5.26** : How many ways to distribute four distinct objects into three distinguishable containers **with no container empty**? How many ways to distribute four distinct objects into three identical containers with no container empty?
  - Solution

    (i) take the problem as counting the number of onto functions $f : A \to B$

    where $|A| = 4, |B| = 3$, $\sum_{k=0}^{3} (-1)^k \binom{3}{3-k} (3-k)^4 = 36$

    (ii) Consider the following collections under the distinct containers

    (1) $\{a,b\}_1 \ \{c\}_2 \ \{d\}_3$ (2) $\{a,b\}_1 \ \{d\}_2 \ \{c\}_3$

    (3) $\{c\}_1 \ \{a,b\}_2 \ \{d\}_3$ (4) $\{c\}_1 \ \{d\}_2 \ \{a,b\}_3$

    (5) $\{d\}_1 \ \{a,b\}_2 \ \{c\}_3$ (6) $\{d\}_1 \ \{c\}_2 \ \{a,b\}_3$

    Now if the containers are identical, these $6 = 3!$ distributions are the same.

    $\therefore$ there are $\frac{36}{3!} = 6$ ways.

Onto Functions: Stirling Numbers of the Second Kind

- General formulas:

  $\sum_{k=0}^{n}(-1)^k\binom{n}{n-k}(n-k)^m$ ways to distribute m distinct objects into $\underline{n \text{ numbered containers}}$.

  $\frac{1}{n!}\sum_{k=0}^{n}(-1)^k\binom{n}{n-k}(n-k)^m$ ways to distribute m distinct objects into $\underline{n \text{ identical containers}}$.

  This will be donated by $\underline{S(m,n)}$ and is called a Stirling number of the second kind.

- Note that for |A|=m ≥ n = |B|, there ***n!*S(m, n)*** onto functions from A to B.

- **Ex 5.27**:

  For $m \geq n, \sum_{i=1}^{n} S(m,i)$ is the number of possible ways to distribute m distinct objects into n identical containers with empty containers allowed.

More Stirling Numbers of the 2^{nd} Kind

- The number of ways of partitioning a set of m elements into n **nonempty** sets denoted $S(m,n)$
- Example: The set {1,2,3} can be partitioned
  - into three subsets in one way(S(3,3)):{{1},{2},{3}} ;
  - into two subsets in three ways(S(3,2)): {{1},{2,3}} , {{1,3},{2}} , and {{1,2},{3}} ;
  - into one subset in one way(S(3,1)): {{1,2,3}} .
- The Stirling numbers of the second kind for three elements are S(3,1)=1, S(3,2)=3, S(3,3)=1.
- http://mathworld.wolfram.com/StirlingNumberoftheSecondKind.html

More Stirling Numbers of the 2nd Kind

- For positive integers m,n with *m*<*n*, prove that

$$\sum_{k=0}^{n}(-1)^k\binom{n}{n-k}(n-k)^m=0$$

- For every positive integer n, verify that

$$n!=\sum_{k=0}^{n}(-1)^k\binom{n}{n-k}(n-k)^n$$

Onto Functions: Stirling Numbers of the Second Kind

- Theorem 5.3: Let $m \geq n > 1$, then $S(m+1,n) = S(m,n-1) + n \cdot S(m,n)$
  - **Proof**

    Let $A = \{a_1, a_2, \cdots, a_m, a_{m+1}\}$. Then $S(m+1,n)$ counts the number of ways in which the objects of A can be distributed among n identical containers, with no container left empty.

    (1) (i) $S(m,n-1)$ ways of distributing $a_1, a_2, \cdots, a_m$ objects among $n-1$ identical containers

    (ii) 1 selection of placing a_{m+1} in the remaining empty (nth) container

    $\Rightarrow S(m,n-1)$ ways

    (2) (i) $S(m,n)$ ways of distributing $a_1, a_2, \cdots, a_m$ objects among n identical containers

    (ii) n selection of placing a_{m+1} in the n identical containers

    $\Rightarrow nS(m,n)$ ways

    $\therefore$ Totally, $S(m+1,n) = S(m,n-1) + nS(m,n)$
- Example:

$$m = 7, n = 3$$

$$\Rightarrow S(7+1,3) = 966 = 63 + 3 \cdot 301 = S(7,2) + 3S(7,3)$$

Onto Functions: Stirling Numbers of the Second Kind

- Alternative form: $\frac{1}{n}[n!S(m+1,n)] = (n-1)!S(m,n-1) + n!S(m,n)$
- This new form tells something about the number of onto functions.

Let $A = \{a_1, a_2, \cdots, a_m, a_{m+1}\}, B = \{b_1, b_2, \cdots, b_{n-1}, b_n\}$.

$\left(\frac{1}{n}\right)$(the number of onto functions $h: A \to B$)

$=$(the number of onto functions $f: A-\{a_{m+1}\} \to B-\{b_n\}$)$+$(the number of onto functions $g: A-\{a_{m+1}\} \to B$)

5.4 Special Functions

- Definition 5.10: For any nonempty sets A, B, any function $f : A \times A \to B$ is called a binary operation on A. If $B \subseteq A$, then the binary operation is said to be closed (on A).
- Definition 5.11: A function $g : A \to A$ is called a unary (monary) operation on A.

- **Ex 5.29**:

(a) The function $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$, defined by $f(a,b) = a - b$, is a closed binary operation on $\mathbf{Z}$.

(b) If $g : \mathbf{Z}^+ \times \mathbf{Z}^+ \to \mathbf{Z}$ is the function where $g(a,b) = a - b$, then g is a binary operation on $\mathbf{Z}^+$ but it is not closed. for example, we find that $3,7 \in \mathbf{Z}^+$, but $g(3,7) = 3 - 7 = -4 \notin \mathbf{Z}^+$.

(c) The function $h : \mathbf{R}^+ \to \mathbf{R}^+$ defined by $h(a) = \frac{1}{a}$ is a unary operation on $\mathbf{R}^+$.

Special Functions

- **Ex 5.30** : Let U be a universe, and $A,B \subseteq U$
  (a) If $f: P(U) \times P(U) \to P(U)$ is defined by $f(A,B) = A \cup B$, then f is a closed binary operation on $P(U)$.
  (b) The function $g: P(U) \to P(U)$ is defined by $g(A) = \overline{A}$ is a unary operation on $P(U)$.

- Definition 5.12: Let $f: A \times A \to B$, i.e., f is a binary operation on A.
  (a) f is said to be commutative if $f(a,b) = f(b,a)$ for all $(a,b) \in A \times A$,
  (b) When $B \subseteq A$, f is said to be associative if all $a,b,c \in A$,
  $f(f(a,b),c) = f(a, f(b,c))$.

- **Ex 5.31** :
  (a) $f(A,B) = A \cup B$ (Example 5.30) is commutative and associative.
  (b) $f(a,b) = a - b$ (Example 5.29) neither.

Example

- $f: Z \times Z \rightarrow Z$, by $f((x,y))=x+y-3xy$
  Then $f(x,y)= x+y-3xy=y+x-3yx=f(y,x)$
  Hence f is commutative

- $f((x,y),z)=(x+y-3xy)+z-3(x+y-3xy)z$
  $=x+(y+z-3yz)-3x(y+z-3yz)$
  $=f(x,(y,z))$
  Hence f is associative

Special Functions

- Definition 5.14:

  $D \subseteq A \times B, \pi_A : D \to A$, defined by $\pi_A(a,b) = a$, is called the projection on the first coordinate.

  $\pi_B : D \to B$, defined by $\pi_B(a,b) = b$, is called the projection on the second coordinate.

- **Ex 5.36** :

  If $A = \{w, x, y\}, B = \{1,2,3,4\}, D = \{(x,1),(x,2),(x,3),(y,1),(y,4)\}$

  The projection $\pi_A : D \to A$ satisfies $\begin{cases} \pi_A(x,1) = \pi_A(x,2) = \pi_A(x,3) = x \\ \pi_A(y,1) = \pi_A(y,4) = y \end{cases}$

  π_A is not onto, $\because \pi_A(D) = \{x, y\} \neq A$

  The projection $\pi_B : D \to B$ satisfies $\begin{cases} \pi_B(x,1) = \pi_B(y,1) = 1 \\ \pi_B(x,2) = 2 \\ \pi_B(x,3) = 3 \\ \pi_B(y,4) = 4 \end{cases}$

  π_B is onto, $\because \pi_B(D) = \{1,2,3,4\} = B$

Special Functions

- **Ex 5.37** :

  If $A = B = \mathbf{R}, D \subseteq A \times B$ where $D = \{(x, y) \mid y = x^2\}$

  $\because$ The projection $\pi_A(D) = \mathbf{R}$

  $\therefore \pi_A$ is onto

  $\because$ The projection $\pi_B(D) = [0, \infty) \subset \mathbf{R}$

  $\therefore \pi_B$ is not onto

- Extension of Projection

  Let $A_1, A_2, \cdots, A_n$ be sets, $\{i_1, i_2, \cdots, i_m\} \subseteq \{1, 2, \cdots, n\}$ with $i_1 < i_2 < \cdots < i_m, m < n$

  If $D \subseteq A_1 \times A_2 \times \cdots \times A_n = \times_{i=1}^{n} A_i$, then $\pi : D \to A_{i_1} \times A_{i_2} \times \cdots \times A_{i_m}$

  $\pi(a_1, a_2, \cdots, a_n) = (a_{i_1} \times a_{i_2} \times \cdots \times a_{i_m})$ is the projection of D on i_1th, i_2th, $\cdots$, i_mth coordinates

  The elements of D are called *n-tuples*; an element in π(D) is an *m-tuples*.

Special Functions

- These projections arise in a natural way in the study of relational data bases, a standard technique for organizing and describing large quantities of data by modern large-scale computing systems.
- **Ex 5.38** : At a certain university the following sets are related for purposes of registration:
  A_1 = the set of course numbers for courses offered in mathematics.
  A_2 = the set of course titles offered in mathematics.
  A_3 = the set of mathematics faculty.
  A_4 = the set of letters of the alphabet.
- Consider the table (relation), $D \subseteq A_1 \times A_2 \times A_3 \times A_4$

Course Number	Course Title	Professor	Section Letter
MA 111	Calculus I	P. Z. Chinn	A
MA 111	Calculus I	V. Larney	B
MA 112	Calculus II	J. Kinney	A
MA 113	Calculus III	A. Schmidt	A

Special Functions

- The sets A_1, A_2, A_3, A_4 are called the domain of relational data base, and table D is said have degree 4.
- Each element of D is often called a list (record).
- The projections of D on $A_1 \times A_3 \times A_4$, and $A_1 \times A_2$ is shown in the following tables.

Course Number	Professor	Section Letter
MA 111	P. Z. Chinn	A
MA 111	V. Larney	B
MA 112	J. Kinney	A
MA 113	A. Schmidt	A

Course Number	Course Title
MA 111	Calculus I
MA 112	Calculus II
MA 113	Calculus III

5.6 Function Composition and Inverse Functions

- Definition 5.15: If $f: A \to B$, then f is said to be bijective, or to be a one-to-one correspondence, if f is one-to-one and onto.
- **Ex 5.50** : $A = \{1, 2, 3, 4\}$, $B = \{w, x, y, z\}$, $f = \{(1, w), (2, x), (3, y), (4, z)\}$, $g = \{(w, 1), (x, 2), (y, 3), (z, 4)\}$ are one-to-one correspondences from A (on)to B / from B (on)to A.

- Definition 5.16:
  Identity function : $1_A : A \to A$, defined by $1_A(a) = a$ for all $a \in$ A
- Definition 5.17:
  $f, g: A \to B$, f, g are equal $(f = g)$ if $f(a) = g(a)$ for all $a \in A$

Denoted 1_A or id_A
Identity Matrix I_n

Function Composition and Inverse Functions

- **Ex 5.52** :

  $$f,g:\mathbf{R}\to\mathbf{Z},\ f(x)=\begin{cases} x, & \text{if } x\in\mathbf{Z} \\ \lfloor x\rfloor+1, & \text{if } x\in\mathbf{R}-\mathbf{Z}\end{cases},\ g(x)=\lceil x\rceil \text{ for all } x\in\mathbf{R}$$

  show that f and g are equal.

  - Proof

  If $x\in\mathbf{Z}$, then $f(x)=x=\lceil x\rceil=g(x)$

  If $x\in\mathbf{R}-\mathbf{Z}$, write $x=n+r$ where $n\in\mathbf{Z}$ and $0<r<1$, then

  $f(x)=\lfloor x\rfloor+1=n+1=\lceil x\rceil=g(x)$

Function Composition and Inverse Functions

- Definition 5.18: The composite function,
  If $f : A \to B$ and $g : B \to C$, then $g \circ f : A \to C$,
  by $(g \circ f)(a) = g\,(f\,(a))$, for all $a \in A$.

- g o f is read as "g circle f" or "g composed with f"

- **Ex 5.53** :

  Let $f : \mathbf{R} \to \mathbf{R}$, $g : \mathbf{R} \to \mathbf{R}$, $f(x) = x^2, g(x) = x + 5$.

  Then $(g \circ f)(x) = g\,(f\,(x)) = g(x^2) = x^2 + 5$

  whereas $(f \circ g)(x) = f\,(g(x)) = f\,(x+5) = (x+5)^2 = x^2 + 10x + 25$.

  $\therefore$ not commutative

Function Composition and Inverse Functions

- Theorem 5.5: Let $f : A \to B$ and $g : B \to C$.

  a) If f and g are one-to-one, then $g \circ f$ is one-to-one.

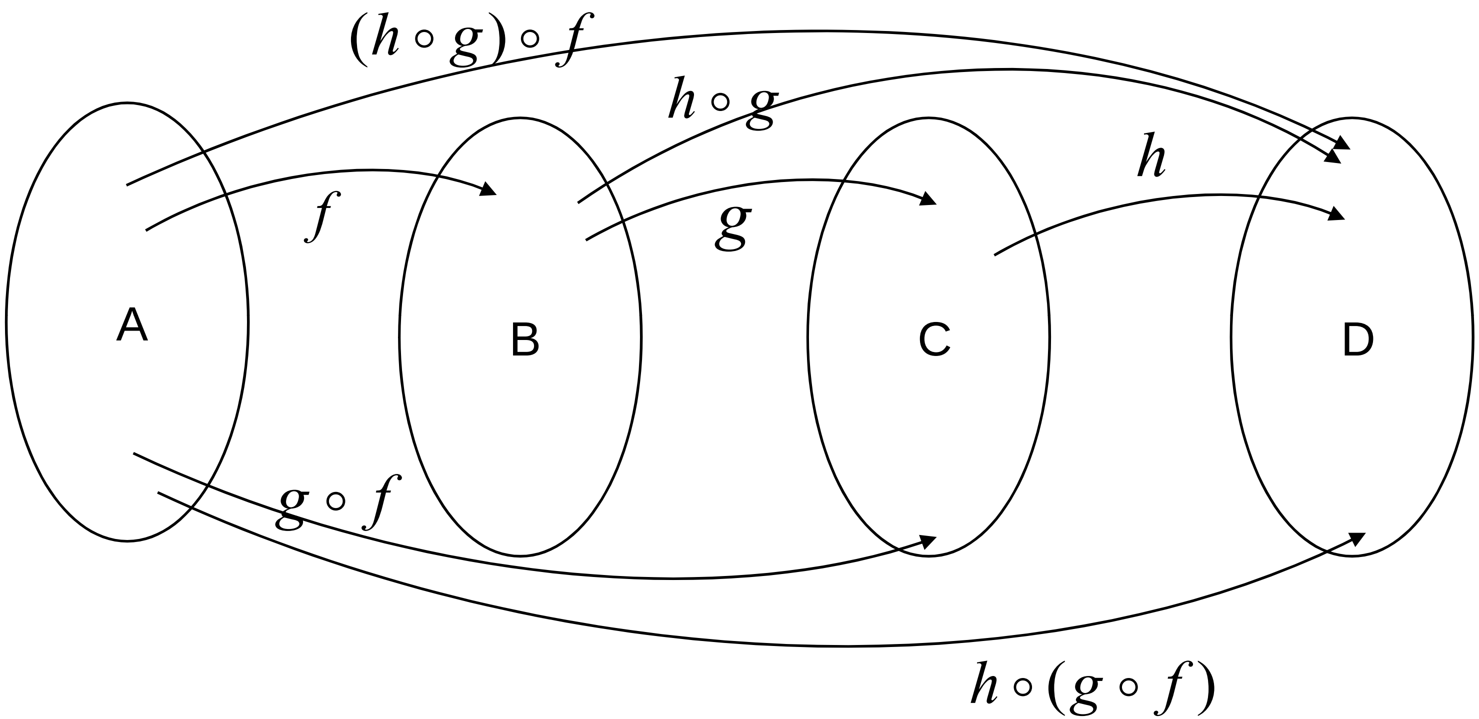
  b) If f and g are onto, then $g \circ f$ is onto.

  - Proof

$$
\begin{aligned}
&\text{a) Let } a_1, a_2 \in A \text{ with } (g \circ f)(a_1) = (g \circ f)(a_2) \\
&\quad \Rightarrow g(f(a_1)) = g(f(a_2)) \Rightarrow f(a_1) = f(a_2) (\because g \text{ is one-to-one}) \\
&\quad \Rightarrow a_1 = a_2 (\because f \text{ is one-to-one}) \\
&\quad \therefore g \circ f \text{ is one-to-one} \\
&\text{b) For } g \circ f : A \to C, \text{ let } z \in C \\
&\quad \because g \text{ is onto}, \therefore \text{ exists } y \in B \text{ with } g(y) = z \\
&\quad \because f \text{ is onto}, \therefore \text{ exists } x \in A \text{ with } f(x) = y \\
&\quad \therefore z = g(y) = g(f(x)) = g \circ f(x) \\
&\quad \therefore g \circ f \text{ is onto}
\end{aligned}
$$

Function Composition and Inverse Functions

- Theorem 5.6: Let $f: A \to B, g: B \to C$, and $h: C \to D$, then $(h \circ g) \circ f = h \circ (g \circ f)$. (associative)



Function Composition and Inverse Functions

- Definition 5.19:
  If $f: A \to A$, we define $f^1 = f$, and for $n \in \mathbf{Z}^+$, $f^{n+1} = f \circ (f^n)$.

- **Ex 5.56** :
  $A = \{1,2,3,4\}$, $f: A \to A$, and $f = \{(1,2),(2,2),(3,1),(4,3)\}$
  $f^2 = f \circ f = \{(1,2),(2,2),(3,2),(4,1)\}$, $f^3 = f \circ f^2 = \{(1,2),(2,2),(3,2),(4,2)\}$
  What are f^4, f^5?

- Definition 5.20:
  For sets A, B, if $\Re$ is a relation from A to B, then the converse of $\Re$,
  denoted $\Re^c$, is the relation from B to A denoted by $\Re^c = \{(b,a) \mid (a,b) \in \Re\}$.

- **Ex 5.57** :
  $A = \{1,2,3\}$, $B = \{\mathrm{w}, \mathrm{x}, \mathrm{y}\}$, $f: A \to B$, and $f = \{(1,w),(2,x),(3,y)\}$
  $\Rightarrow f^c = \{(w,1),(x,2),(y,3)\} \Rightarrow f^c \circ f = 1_A, f \circ f^c = 1_B$

Function Composition and Inverse Functions

- Definition 5.21:
  If $f : A \to B$, then f is said to be invertible, if there is function $g : B \to A$, such that $g \circ f = 1_A$ and $f \circ g = 1_B$.
- **Ex 5.58** : Let $f, g : \mathbf{R} \to \mathbf{R}$ with $f(x) = 2x + 5, g(x) = \frac{x-5}{2}$

  Then $(g \circ f)(x) = g(f(x)) = g(2x+5) = \frac{(2x+5)-5}{2} = x$

  $(f \circ g)(x) = f(g(x)) = f(\frac{x-5}{2}) = 2(\frac{x-5}{2}) + 5 = x$

  $\therefore f \circ g = 1_{\mathbf{R}}, g \circ f = 1_{\mathbf{R}}$, f and g are both invertible functions
- Theorem 5.7: If $f : A \to B$ is invertible and $g : B \to A$ satisfies $g \circ f = 1_A$ and $f \circ g = 1_B$, then g is unique.
  - Proof

    If g is not unique, then there is another function $h : B \to A$ with $h \circ f = 1_A$ and $f \circ h = 1_B$, then

    $h = h \circ 1_B = h \circ (f \circ g) = (h \circ f) \circ g = 1_A \circ g = g.$

Function Composition and Inverse Functions

- Theorem 5.8: $f: A \to B$ is invertible $\Leftrightarrow$ it is one-to-one and onto.
  - **Proof**

    (1) Assuming that $f: A \to B$ is invertible, and exists unique $g: B \to A$ with

    $g \circ f = 1_A,\ f \circ g = 1_B$

    (i) one-to-one: if $a_1, a_2 \in A$ with $f(a_1) = f(a_2) \Rightarrow g(f(a_1)) = g(f(a_2))$

    i.e., $(g \circ f)(a_1) = (g \circ f)(a_2), \because g \circ f = 1_A, \therefore a_1 = a_2$

    (ii) onto: let $b \in B \Rightarrow g(b) \in A$

    $b = 1_B(b) = (f \circ g)(b) = f(g(b)), \therefore f$ is onto

    ---

    (2) Suppose $f: A \to B$ is bijective

    $\because f$ is onto, $\therefore$ each $b \in B$ with $f(a) = b$

    define $g: B \to A$ by $g(b) = a$, where $f(a) = b$

    consider the possible problem $g(b) = a_1 \neq a_2 = g(b)(\because f(a_1) = b = f(a_2))$

    $\because f$ is one-to-one $\therefore$ this situation cannot arise

    $\therefore g \circ f = 1_A,\ f \circ g = 1_B$

    $\therefore f$ is invertible

Function Composition and Inverse Functions

- **Ex 5.59** :
  $f_1 : \mathbf{R} \to \mathbf{R}$ defined by $f_1(x) = x^2$ is not invertible

  $f_2 : [0,+\infty) \to [0,+\infty)$ defined by $f_2(x) = x^2$ is invertible with $f_2^{-1}(x) = \sqrt{x}$

  $*$ We call the function f^{-1} the inverse of f.
- Theorem 5.9: If $f : A \to B$, $g : B \to C$ are invertible functions, then $g \circ f : A \to C$ is invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. ($f^{-1}$ is the inverse of f)
- **Ex 5.60** :
  For $m, b \in \mathbf{R}, m \neq 0$, $f : \mathbf{R} \to \mathbf{R}$, defined by $f = \{(x, y) \mid y = mx + b\}$ is invertible because it is one-to-one and onto, and $f^{-1}(x) = \frac{x-b}{m}$.
- **Ex 5.61** :
  $f : \mathbf{R} \to \mathbf{R}^+$ defined by $f(x) = e^x$ is invertible, $f^{-1}(x) = \ln x$

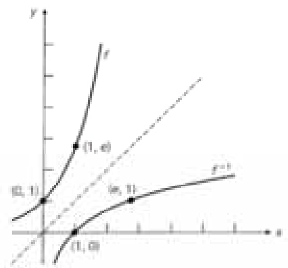


Figure 5.10

Function Composition and Inverse Functions

- Definition 5.22:

  If $f: A \to B$ and $B_1 \subseteq B$, then $f^{-1}(B_1) = \{x \in A \mid f(x) \in B_1\}$

  $f^{-1}(B_1)$ is called the preimage of B_1 under f. *(f is not necessary invertible.)*

- **Ex 5.62** :

  Let $A = \{1,2,3,4,5,6\}$, $B = \{6,7,8,9,10\}$. If $f: A \to B$ *with*

  $f = \{(1,7),(2,7),(3,8),(4,6),(5,9),(6,9)\}$, then the following results are obtained.

  a) For $B_1 = \{6,8\} \subseteq B$, $f^{-1}(B_1) = \{3,4\}$, $|f^{-1}(B_1)| = 2 = |B_1|$

  e) For $B_5 = \{8,10\}$, $f^{-1}(B_5) = \{3\}(\because f(3) = 8, f^{-1}(\{10\}) = \phi$, $|f^{-1}(B_5)| = 1 < 2 = |B_5|$

Function Composition and Inverse Functions

- Theorem 5.10:
  If $f: A \to B$ and $B_1, B_2 \subseteq B$, then (a) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$

  (b) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$

  - **Proof**

    (b) If $a \in A, a \in f^{-1}(B_1 \cup B_2) \Leftrightarrow f(a) \in B_1 \cup B_2$

    $\Leftrightarrow f(a) \in B_1$ or $f(a) \in B_2 \Leftrightarrow a \in f^{-1}(B_1)$ or $a \in f^{-1}(B_2)$

    $\Leftrightarrow a \in f^{-1}(B_1) \cup f^{-1}(B_2)$

- Theorem 5.11:

  Let $f: A \to B$ for finite sets A and B, where $|A| = |B|$.

  Then the following statements are equivalent :

  (a) f is one-to-one; (b) f is onto; (c) f is invertible.

Function Composition and Inverse Functions

- Problem 6: For every positive integer *n*, verify that

$$n! = \sum_{k=0}^{n} (-1)^k \binom{n}{n-k} (n-k)^n.$$

  - **Proof**

    $\because |A| = |B| = n \therefore$ there are $n!$ one - to - one functions, and

    $\sum_{k=0}^{n} (\text{-}1)^k \binom{n}{n-k} (n\text{-}k)^n$ onto functions

    Using Theorem 5.11(a) and (b) $\Rightarrow n! = \sum_{k=0}^{n} (\text{-}1)^k \binom{n}{n-k} (n\text{-}k)^n$

    Thus, $S(n,n) = \frac{1}{n!} \sum_{k=0}^{n} (\text{-}1)^k \binom{n}{n-k} (n\text{-}k)^n = 1.$

Reference

- $A=\{a_1,a_2,\ldots,a_m\}, B=\{b_1,b_2,\ldots,b_n\}$, and $m \le n$, there are

  a) 2^{mn} realtions from A to B

  b) n^m functions from A to B

  c) $P(n,m)=n(n-1)(n-2)\cdots(n-m+1)$ one - to - one functions from A to B

  d) onto function : $\sum_{k=0}^{n}(-1)^k\binom{n}{n-k}(n-k)^m$ ways

  to distribute m distinct objects into n numbered containers.

  e) Stirling number : $S(m,n)=\frac{1}{n!}\sum_{k=0}^{n}(-1)^k\binom{n}{n-k}(n-k)^m$ ways

  to distribute m distinct objects into n identical containers.

Reference: Counting Principles

- Table 5.13

Objects Are Distinct	Containers Are Distinct	Some Container(s) May Be Empty	Number of Distributions
Yes	Yes	Yes	n^m
Yes	Yes	No	$n!\,S(m, n)$
Yes	No	Yes	$S(m, 1) + S(m, 2) + \cdots + S(m, n)$
Yes	No	No	$S(m, n)$
No	Yes	Yes	$\binom{n+m-1}{m}$
No	Yes	No	$\binom{n+(m-n)-1}{(m-n)} = \binom{m-1}{m-n} = \binom{m-1}{n-1}$

5.7 Computational Complexity

- Properties of a general algorithm
  - Precision of the individual step-by-step instructions
  - Input provided to the algorithm, and the output the algorithm then provides
  - Ability of the algorithm to solve a certain type of problem, not just specific instances of the problem
  - Uniqueness of the intermediate and final results, based on the input
- Examining an algorithm
  - Measure how long it takes the algorithm to solve a problem of a large size
  - Determine whether one algorithm is better than another
- To measure an algorithm means seeking a function $f(n)$, called the <u>time-complexity function</u>.

Computational Complexity

- Definition 5.23:

  Let $f, g : \mathbf{Z}^+ \to \mathbf{R}$. We say that g dominates f if there exist constants $m \in \mathbf{R}^+$ and $k \in \mathbf{Z}^+$ such that $|f(n)| \le m|g(n)|$ for all $k \in \mathbf{Z}^+$, where $n \ge k$.

  - "Big-Oh" notation, we write

    $f \in O(g)$, where $O(g)$ is read "order g" or "big-Oh of g".

    $O(g)$ represents the set of all functions with domain $\mathbf{Z}^+$ and codomain R that are dominated by g.

- **Ex 5.65** :

  Let $f, g : \mathbf{Z}^+ \to \mathbf{R}$ be given by $f(n) = 5n, g(n) = n^2$, for $n \in \mathbf{Z}^+$.

  (i) $1 \le n \le 4 : f(1) = 5, g(1) = 1; f(2) = 10, g(2) = 4; f(3) = 15,$
  $f(3) = 9; f(4) = 20, g(4) = 16$

  (ii) $n \ge 5 : n^2 \ge 5n, \therefore m = 1, k = 5, |f(n)| \le m|g(n)|$ for $n \ge k$.

  $\therefore g$ dominates f and $f \in O(g)$

Computational Complexity

- **Ex 5.67** :

  Let $f, g : \mathbf{Z}^+ \to \mathbf{R}$ with $f(n) = 5n^2 + 3n + 1, g(n) = n^2$.

  $|f(n)| = |5n^2 + 3n + 1| = 5n^2 + 3n + 1 \le 5n^2 + 3n^2 + n^2 = 9n^2 = 9|g(\text{n})|$

  $\therefore |f(n)| \le m|g(n)|$ for any $m \ge 9, f \in O(g)$ or $f \in O(n^2)$.

- Generalization of function dominance

  Let $f, g : \mathbf{Z}^+ \to \mathbf{R}$ with $f(n) = a_t n^t + a_{t-1} n^{t-1} + \cdots + a_1 n + a_0$

$$
\begin{aligned}
|f(n)| &= |a_t n^t + a_{t-1} n^{t-1} + \cdots + a_1 n + a_0| \\
&\le |a_t n^t| + |a_{t-1} n^{t-1}| + \cdots + |a_1 n| + |a_0| \\
&= |a_t| n^t + |a_{t-1}| n^{t-1} + \cdots + |a_1| n + |a_0| \\
&\le |a_t| n^t + |a_{t-1}| n^t + \cdots + |a_1| n^t + |a_0| n^t \\
&= (|a_t| + |a_{t-1}| + \cdots + |a_1| + |a_0|) n^t
\end{aligned}
$$

  Let $m = |a_t| + |a_{t-1}| + \cdots + |a_1| + |a_0|, k = 1, g(n) = n^t$

  $\Rightarrow f(n) \le m|g(n)|, f \in O(n^t)$

Computational Complexity

- **Ex 5.68** :

(a) Let $f:\mathbf{Z}^+ \to \mathbf{R}$ be given by $f(n) = 1 + 2 + \cdots + n$.

$f(n) = \frac{1}{2} \cdot n \cdot (n+1) = (\frac{1}{2})n^2 + (\frac{1}{2})n, \therefore f \in O(n^2)$

(b) Let $g:\mathbf{Z}^+ \to \mathbf{R}$ with $g(n) = 1^2 + 2^2 + \cdots + n^2$.

$g(n) = \frac{1}{6} \cdot n \cdot (n+1)(2n+1) = (\frac{1}{3})n^3 + (\frac{1}{2})n^2 + (\frac{1}{2})n, \therefore g \in O(n^3)$

(c) If $h:\mathbf{Z}^+ \to \mathbf{R}$ is defined by $h(n) = \sum_{i=1}^{n} i^t$.

then $h(n) = 1^t + 2^t + \cdots + n^t \le n^t + n^t + \cdots + n^t = nn^t = n^{t+1}$,

$\therefore h \in O(n^{t+1})$

Computational Complexity

- Some important orders:

Big-Oh Form	Name
$O(1)$	Constant
$O(\log_2 n)$	Logarithmic
$O(n)$	Linear
$O(n \log_2 n)$	$n \log_2 n$
$O(n^2)$	Quadratic
$O(n^3)$	Cubic
$O(n^m)$	Polynomial
$O(c^n), c > 1$	Exponential
$O(n!)$	Factorial

Ω and Θ

Exercise 5.7, Questions 11 and 14:

Let f and g be functions from Z^+ to R.

The function f is of *order at least* g if and only if there are $M \in R^+$ and an $k \in N^+$ such that $|f(n)| \geq M\,|g(n)|$ for all $k \leq n$.

This is denoted by $f \in \Omega(g)$.

Say: "f is/has order big-Omega of g"

If $f \in O(g)$ and $f \in \Omega(g)$, then we can write $f \in \Theta(g)$

In words: "f has order big-Theta of g"

Examples: $n^2 \in \Omega(n)$ and $7n^2 - 8n + 10 \in \Theta(n^2)$ and

$2^n \in \Omega(n^c)$ for every c.

Big-O, Ω and Θ

Definitions:

If f is dominated by g: $f \in O(g)$

Equivalently: $g \in \Omega(f)$.

If $f \in O(g)$ and $g \in O(f)$ then $f \in \Theta(g)$

Some examples:

For polynomials f and g: $f \in O(g)$

if and only if $\deg(f) \leq \deg(g)$.

For all polynomials f and $c \in R>1$: $f \in O(c^n)$

Examples of O, Ω and Θ

- $n^3 \in \Omega(n^2)$
- $2^n \in \Omega(n^c)$ for every finite $c \in R$
- $(\log n)^c \in O(n)$ for every finite $c \in R$
- $n \log n \in \Omega(n)$
- $5n^7 + 6n^5 + 4 \in \Theta(n^7)$
- $2^{\log n} \in \Theta(n)$

- $c^n = 2^{(\log c)n} \in 2^{\Theta(n)}$ for every $c>1$
- $n \log n \in O(n^{1+\varepsilon})$ for every $\varepsilon>0$, but not $\varepsilon=0$

Some More Subtle Cases

The set $O(n^2)$ contains all functions f that do not grow faster than a quadratic polynomial. For cubic polynomials: $O(n^3)$.

Hence: $O(n) \subset O(n^2) \subset O(n^3) \subset O(n^4) \ldots \subset O(2^n)$

How to express the set of all constant degree polynomials?

Answer: $n^{O(1)} = O(n) \cup O(n^2) \cup O(n^3) \ldots$

Similarly for exponential functions: $O(2^n) \subset O(3^n) \subset O(4^n) \ldots$

Rewrite this as $O(2^n) \subset O(2^{\log(3)\cdot n}) \subset O(2^{\log(4)\cdot n}) \ldots$

The set of all such exponential functions is thus $2^{\Theta(n)}$.

Hard versus Easy Problems

Typically we call a problem **easy** if there is a polynomial time algorithm that solves it in time $n^{O(1)}$. If there is no such poly-time algorithm, then we call the problem hard.

Problems for which we only have exponential time algorithms (time complexity $2^{\Theta(n)}$) are very hard…

Take an input of n=256 bits and time complexity 2^n. Observe that $2^n = 2^{256} \approx 10^{77}$ steps on a computer with clock speed 10^{12} operations per second (tera) still requires 10^{65} seconds. (about 9 years)

5.8 Analysis of Algorithm

- **Ex 5.69** : Procedure AccountBalance computes the balance in a saving account n months after it has been opened.
  - **Solution**

$$f(n) = 4 + 7n + 1$$
$$= 7n + 5 \in O(n)$$

```
Procedure AccountBalance (n: integer)
begin
   deposit := 50.00
   I := 1
   rate := 0.05
   balance := 100.00
   while I ≤ n do
      begin
         balance := deposit + balance + balance * rate
         I := I + 1
      end
end
```

Analysis of Algorithm

- **Ex 5.70** : An array of n integers $a_1, a_2, \ldots, a_n$ is to be searched for the presence of an integer called key. If the integer is found, the value of location indicates its first location in the array; if it is not found the value of location is 0, indicating an unsuccessful search. Analyze the complexity of the algorithm.
  - **Solution**

(i) best-case complexity: $O(1)$

(ii) worst-case complexity: $O(n)$

(iii) average-case complexity:

p, q: the probability of key being or not in array

np+q=1

$$f(n) = (1 \cdot p + 2 \cdot p + \cdots + n \cdot p) + n \cdot q$$
$$= \tfrac{pn(n+1)}{2} + nq$$

If $q = 0, p = 1/n \Rightarrow f(n) = (n+1)/2 \in O(n)$

If $q = 1/2, p = 1/2n \Rightarrow$

$$f(n) = (1/2n)n(n+1)/2 + n/2$$
$$= (n+1)/4 + (n/2) \in O(n)$$

```
Procedure LinearSearch (key, n: integer; a1, a2, …, an: integers )
begin
   I := 1
   while (I ≤ n and key = ai) do
      I := I + 1
   if I ≤ n then location := I
   else location := 0
end
```

The average-case complexity = the average number of array elements examined

Analysis of Algorithm

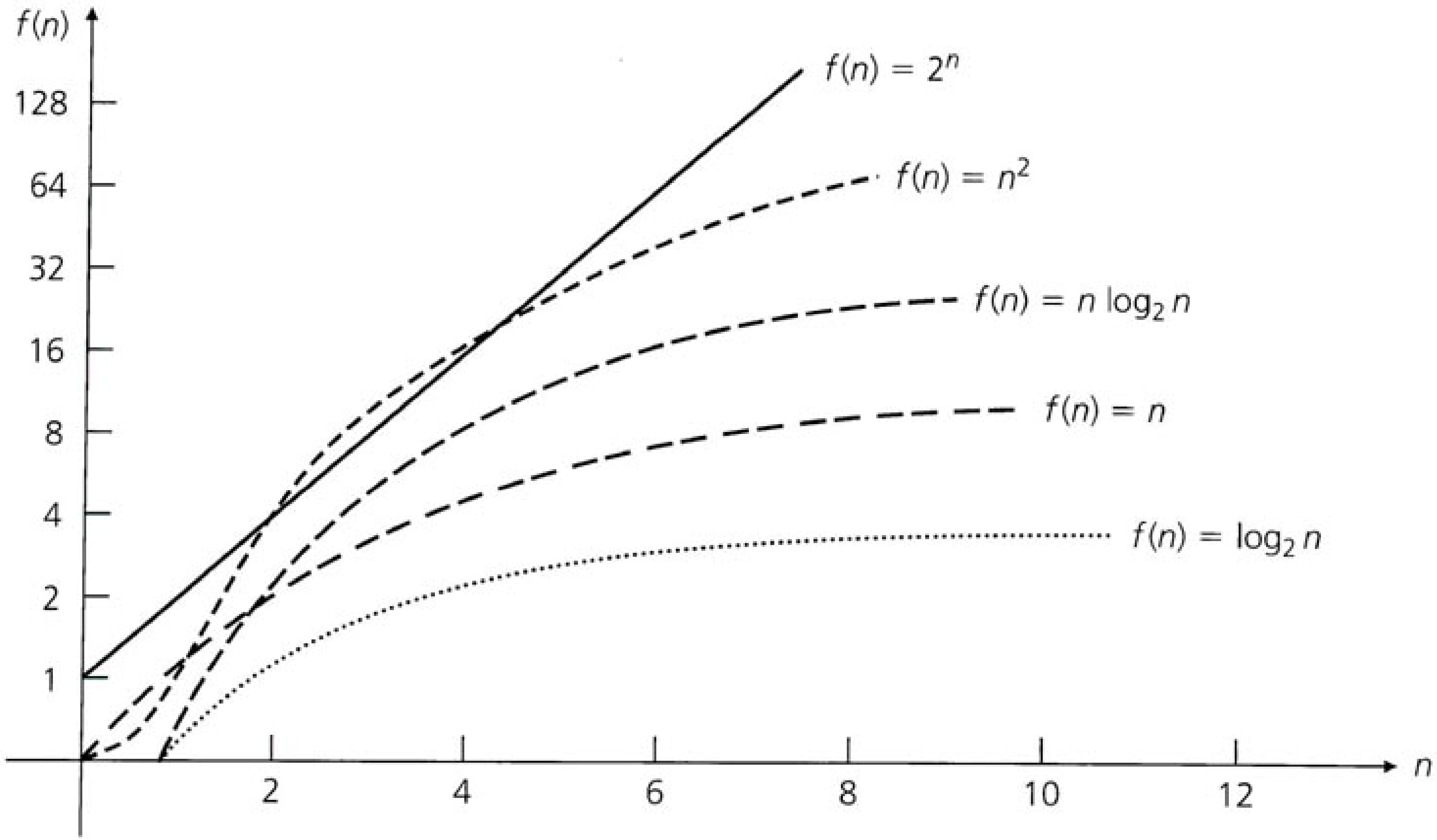


Figure 5.17

Analysis of Algorithm

- Observations

For $f(n) \in O(n)$ and $g(n) \in O(n^2)$, we must be cautious.

We might expect an algorithm with linear complexity to be more efficient than one with quadratic complexity. But we need more information.

If $f(n) = 1000n$ and $g(n) = n^2$, there are different results for $n > 1000$ and $n < 1000$.

Problem size n	Order of Complexity					
	$\log_2 n$	n	n $\log_2 n$	n^2	2^n	n!
2	1	2	2	4	4	2
16	4	16	64	256	$6.5*10^4$	$2.1*10^{13}$
64	6	64	384	4096	$1.84*10^{19}$	$>10^{89}$

$$1.84 \times 10^{19} \text{ microseconds} \approx 2.14 \times 10^8 \text{ days} \approx 5845 \text{centuries}$$