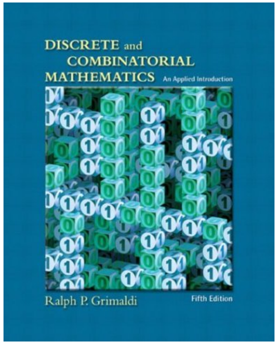
Discrete Mathematics
-- Chapter 5: Relations and Functions



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
- 5.5 The Pigeonhole Principle
- 5.6 Function Composition and Inverse Functions

- 5.7 Computational Complexity
- 5.8 Analysis of Algorithms

Introduction

1) The Defense Department has seven different contracts that deal with a high-security project. Four companies can manufacture the distinct parts called for in each contract, and in order to maximize the security of the overall project, it is best to have all four companies working on some part. In how many ways can the contracts be awarded so that every company is involved?

2) How many seven-symbol quaternary (0, 1, 2, 3) sequences have at least one occurrence of each of the symbols 0, 1, 2, and 3?

3) An $m \times n$ *zero-one matrix* is a matrix A with m rows and n columns, such that in row i, for all $1 \le i \le m$, and column j, for all $1 \le j \le n$, the entry a_{ij} that appears is either 0 or 1. How many 7×4 zero-one matrices have exactly one 1 in each row and at least one 1 in each column? (The zero-one matrix is a data structure that arises in computer science. We shall learn more about it in later chapters.)

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?

5) For positive integers m, n with $m < n$, prove that

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

6) For every positive integer n, verify that

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

七個合約被授予4個公司使得每個公司至少需要一件的方法?

有七個符號四個為一組 (0,1,2,3) 至少每個符號有0,1,2, 和3的方法？

The same problem!

*the number of ways **r** objects be distributed among **n** containers*

	$\boxed{r \text{ distinct}}$	r identical
n distinct	n^r	$C(n+r-1, r)$
$\boxed{n \text{ identical}}$	~~$n^r/n!$~~ X See Chapter 5	See Chapter 9
	$\sum_{i=1}^{n} S(r,i)$	Partitions of integers

5.1 Cartesian Products and Relations

有順序性

- For sets A, B, the Cartesian product (cross product), of A and B is denoted by $A \times B = \{(a,b) \mid a \in A, b \in B\}$. A × B ≠ B × A
  - 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., $(4,5,5) \in B^3$

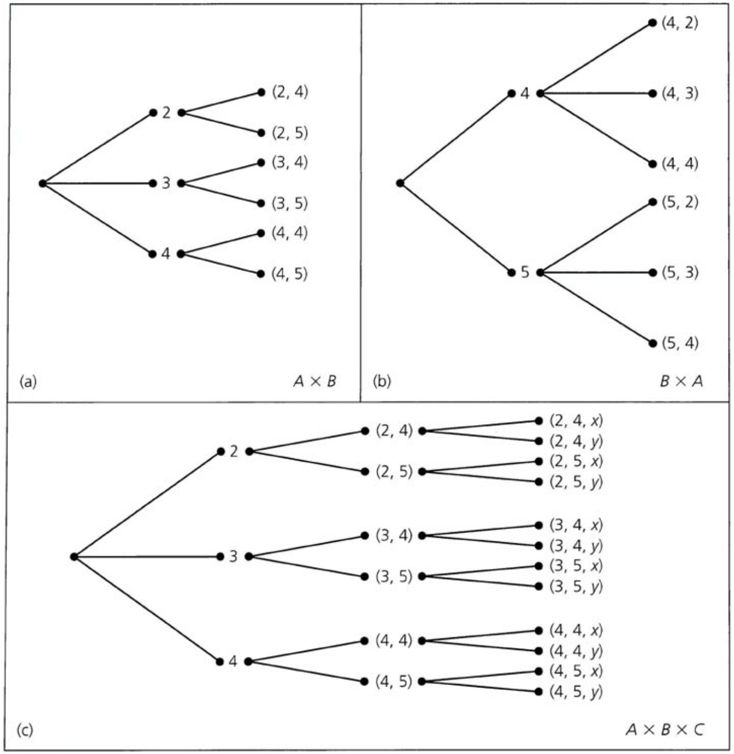


Figure 5.1

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

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)∈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

A × B = mn

- 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 $\{(x, y) \mid x \leq y\}$

  $\Re$ 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 $8 \not\Re 2$

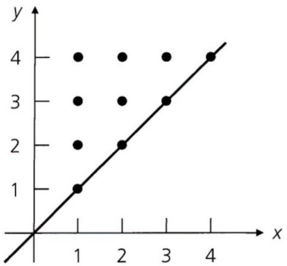


Figure 5.3

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

Cartesian Products and Relations

- Theorem 5.1: For any sets $A, B, C \subseteq \mathscr{U}$:

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

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

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

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

  - Proof

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

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

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

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

5.2: Functions: Plain and One-to-One

較嚴格的relation

- 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 $b = c$. 一個a map到2個 b時，則非function
- **Ex 5.9** :

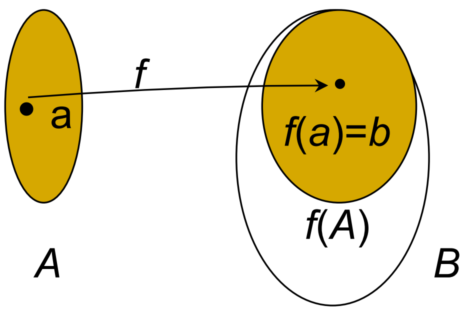
$A = \{1,2,3\}, B = \{w, x, y, z\}$

$f = \{(1, w), (2, x), (3, x)\}$ is a function and a relation

$\mathfrak{R}_1 = \{(1, w), (2, x)\}, \mathfrak{R}_2 = \{(1, w), (2, w), (2, x), (3, z)\}$ are relations, but not functions.

Functions: Plain and One-to-One

- Definition 5.4: Function $f: A \rightarrow B$, A is called the domain of f and B the codomain of f.
  - The subset of B consisting of those elements that appear as second components in the ordered pairs of f is called the range 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 無條件進位

    $g:\mathbf{R}\to\mathbf{Z}, g(x)=\lceil x\rceil=$ 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 無條件捨去
    - $\text{trunc}(3.78)=\lfloor 3.78\rfloor=3, \text{trunc}(-3.78)=\lceil -3.78\rceil=-3$

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

- 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.

  m個n (n個挑m次)

  - 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

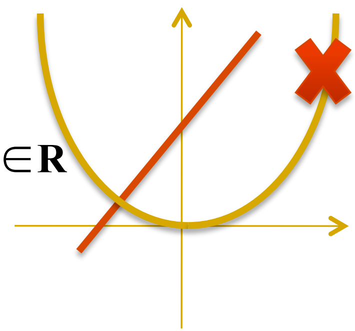
- Definition 5.5: A function $f : A \to B$ is called one-to-one (injective), if each element of B appears at most once as the image of an element of A. element 只出現一次
  - If $f : A \to B$ is one-to-one, with A, B finite, we must have $|A| \leq |B|$.
  - $f : A \to B$ is one-to-one if and only if for all $a_1, a_2 \in A, f(a_1) = f(a_2) \Rightarrow a_1 = a_2$
- **Ex 5.13** :

  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

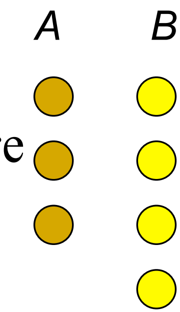
- **Ex 5.13**
  - $$\text{Suppose that } g:\mathbf{R}\rightarrow\mathbf{R} \text{ where } g(x)=x^4-x, \text{ for all } x\in\mathbf{R}$$
    $$g(0)=0^4-0=0 \text{ and } g(1)=1^4-1=0$$
    $$\text{so } g \text{ is not one-to-one } (\because g(0)=g(1) \text{ but } 0\neq 1)$$
- **Ex 5.14**
  - $A=\{1,2,3\}, B=\{1,2,3,4,5\}$

    $f=\{(1,1),(2,3),(3,4)\}$ 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

    $(\because g(2)=g(3) \text{ but } 2\neq 3)$
  - 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

  a > b > c

Functions: Plain and One-to-One

- Definition 5.6:

  If $f: A \rightarrow B$ 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.

- <u>**Ex 5.15**</u> :

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

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

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

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 $A_1 \cap A_2 = \phi$
Or f(a1)=f(a2), but a1,a2 are not the same

- 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 $a \in A_1$. 刪除未map到的relations
- 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. 將多的relations 加入

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.

  => $x \to B=\{1,2,3,4,5\}$

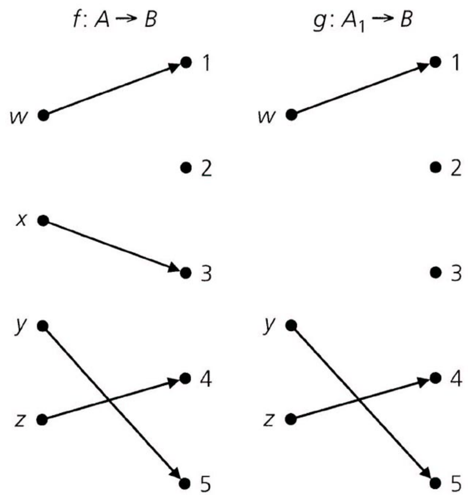


Figure 5.5

5.3 Onto Functions: Stirling Numbers of the Second Kind

需判斷domain　在其對應的domain至少存在一解

- 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 $f(a) = b$.

  一對一、多對1

- **Ex 5.19** :

  How about $f{:}Z \to R$ No

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

  $g: \mathbf{R} \to \mathbf{R}$ with $g(x) = x^2$ is not onto. ex: -1

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

- **Ex 5.20** :

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

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

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

Some Functions

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

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

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?

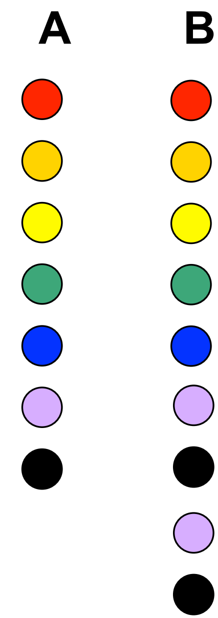
Total number of all functions (trivial): $|B|^{|A|} = n^m$.

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. 無onto function
  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 $f : A \to B$ 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** :

How about B={1,2,3,4}?

|A|=|B|=4, 4! onto functions

$C(4,4)4^4 - C(4,3)3^4 + C(4,2)2^4 - C(4,1)1^4 = 24$

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 :

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

只map到其中2個　非onto function

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 $\{1,2\},\{2,3\},\{1,3\}$ 多扣的

$\therefore$ 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 $|A|=m\ge 3, |B|=3 \Rightarrow \binom{3}{3}3^m - \binom{3}{2}2^m + \binom{3}{1}1^m$ onto functions from A to B 只與 | B | 有關

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 $B = \{w, x, y, z\}$

只map到3個

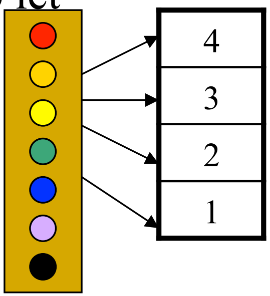
$$\binom{4}{4}4^7 - \binom{4}{3}3^7 + \binom{4}{2}2^7 - \binom{4}{1}1^7$$

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

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**? 工作map到人
  - Solution

Consider two disjoint subcases :

(i) Teresa woks only on the most expensive account

the number of onto functions $f: A \rightarrow B$ 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 $f: C \rightarrow D$ 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?

  onto function

  - Solution

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

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

    (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 n numbered containers.

nonempty

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

This will be donated by $S(m,n)$ 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.

The triangle of Stirling numbers of the second kind

Table 5.1

	$S(m, n)$							
m \ n	1	2	3	4	5	6	7	8
1	1							
2	1	1						
3	1	3	1					
4	1	7	6	1				
5	1	15	25	10	1			
6	1	31	90	65	15	1		
7	1	63	301	350	140	21	1	
8	1	127	966	1701	1050	266	28	1

if $m = 4$, $n = 3$ $S(m+1,n) = S(m,n-1) + n*S(m,n)$

More Stirling Numbers of the 2^{nd} Kind

- The number of ways of partitioning a set of n elements into m **nonempty** sets denoted S(n,m).
- 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

- Since a set of n elements can only be partitioned in a single way into 1 and n subsets
  ➔ $S(n,1)=S(n,n)=1$ 1st column、對角線 = 1

Other special cases include

$$
\begin{aligned}
S(n,0) &= \delta_{n0} \\
S(n,2) &= 2^{n-1}-1 \\
S(n,3) &= \tfrac{1}{6}(3^n - 3\cdot 2^n + 3) \\
S(n,n-1) &= \binom{n}{2}.
\end{aligned}
$$

More Stirling Numbers of the 2nd Kind

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

a map 到 b (| a | = m , | b | = n)

Not onto function

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

- For every positive integer n, verify that

bijection

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

Onto Functions: Stirling Numbers of the Second Kind

容器不能為空

- 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

    先將 m + 1擺到其中1個，將剩下m個擺到n -1個

    (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

    m + 1先不擺，將m個擺到n個，再將m + 1擺到其中1個，但此時m個容器視為不相同

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

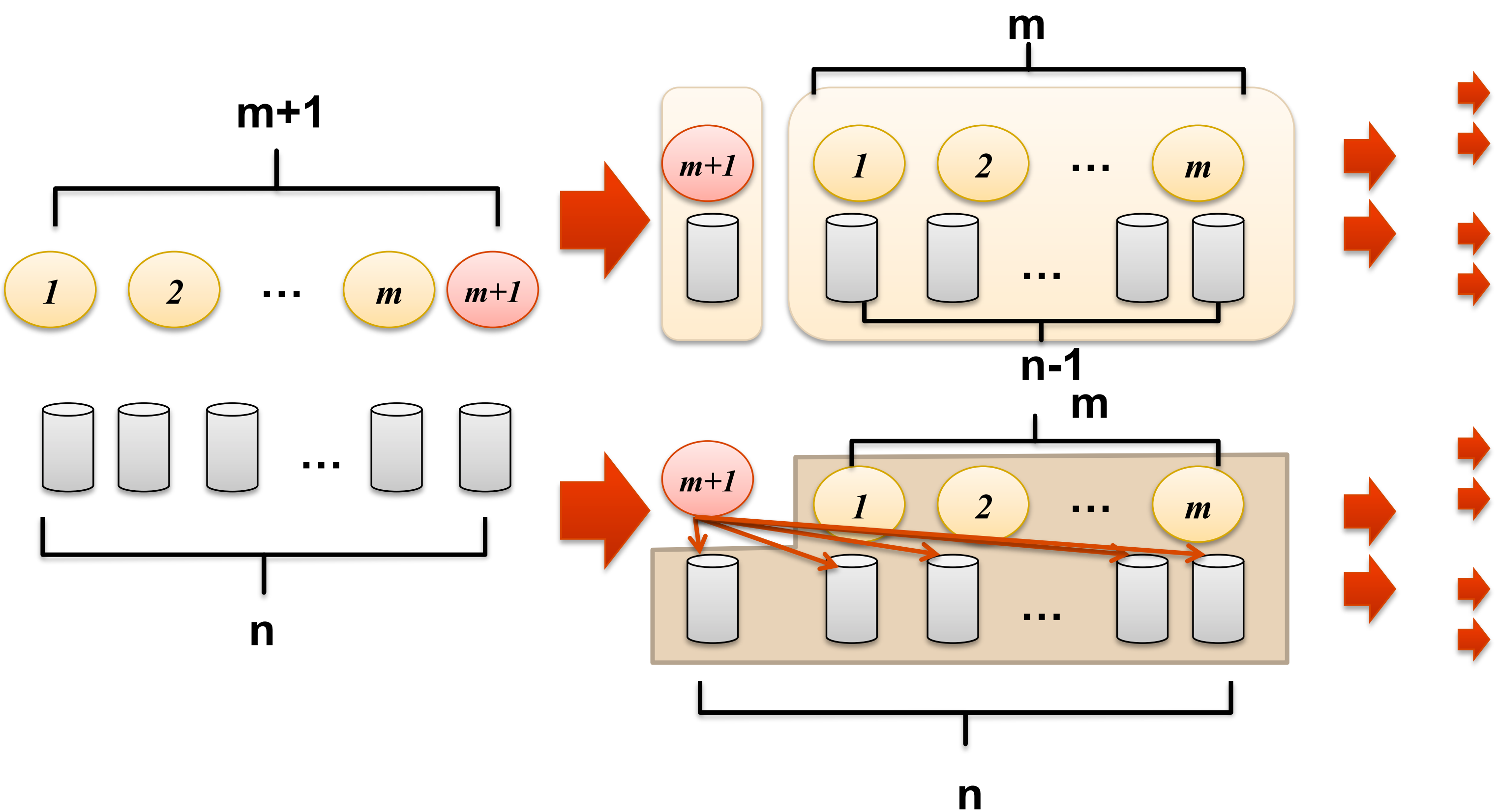
- Example:

$$m = 7, n = 3$$

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

Onto Functions: Stirling Numbers of the Second Kind

Let $m \geq n > 1$, then $S(m+1,n) = S(m,n-1) + n \cdot S(m,n)$



Onto Functions: Stirling Numbers of the Second Kind

$$S(m+1,n) = S(m,n-1) + n \cdot S(m,n)$$

- 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 $g: A - \{a_{m+1}\} \to B$)

- **Ex 5.28** :

  Consider the positive integer $30{,}030 = 2 \times 3 \times 5 \times 7 \times 11 \times 13$

  (i) $30 \times 1001 = (2 \times 3 \times 5)(7 \times 11 \times 13)$

  (ii) $110 \times 273 = (2 \times 5 \times 11)(3 \times 7 \times 13)$

  (iii) $2310 \times 13 = (2 \times 3 \times 5 \times 7 \times 11)(13)$

  (iv) $14 \times 33 \times 65 = (2 \times 7)(3 \times 11)(5 \times 13)$

  (v) $22 \times 35 \times 39 = (2 \times 11)(5 \times 7)(3 \times 13)$

  $*$ $S(6,2) = 31$ ways to factor 30,030 as mn where $m,n \in \mathbf{Z}^+$.

  $*$ $S(6,3) = 90$ ways to factor 30,030 into three integer factors.

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 $f : P(U) \times P(U) \rightarrow P(U)$ is defined by $f(A, B) = A \cup B$, then f is a closed binary operation on $P(U)$.
  (b) The function $g : P(U) \rightarrow P(U)$ is defined by $g(A) = \overline{A}$ is a unary operation on $P(U)$.

- Definition 5.12: Let $f : A \times A \rightarrow B$, 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

- <u>Ex 5.33</u> :

  (1) If $A = \{a,b,c,d\}$, then $|A \times A| = 16 \Rightarrow 4^{16}$ functions $f : A \times A \to A$

  $\Rightarrow 4^{16}$ closed binary operations on A.

  (2) Determine the number of commutative closed binary operations $g(x, y)$ on A.

  (i) $x = y, \{(a,a),(b,b),(c,c),(d,d)\} \to \{a,b,c,d\}$ 對角線

  (ii) $x \neq y$, but $g(x, y) = g(y, x), \frac{16-4}{2} = 6$ sets of two ordered pairs $\to \{a,b,c,d\}$

  上三角、下三角相同（對稱）

  $\therefore$ totally, $4 + 6 = 10$ pairs is available

  $\Rightarrow 4^{10}$ commutative closed binary operations $g(x, y)$ on A.

	a	b	c	d
a	b	c		
b	c			
c				
d				

- Definition 5.13:
  Let $f : A \times A \to B$ be a binary operation on A.

  An element $x \in A$ is called an <u>identity</u> for f if $f(a, x) = f(x, a) = a, \forall a \in A$.

Special Functions

- **Ex 5.34** :

(a) $f:\mathbf{Z}\times\mathbf{Z}\to\mathbf{Z}$, where $f(a,b)=a+b$.

$\Rightarrow$ 0 is an identity, $\because f(a,0)=f(0,a)=a, \forall a$.

(b) $f:\mathbf{Z}\times\mathbf{Z}\to\mathbf{Z}$, where $f(a,b)=a-b$.

$\Rightarrow$ no identity

(c) $g: A\times A\to A$, $A=\{1,2,3,4,5,6,7\}$, where $g(a,b)=\min\{a,b\}$.

$\Rightarrow$ 7 is an identity, $\because g(a,7)=\min\{a,7\}=a=\min\{7,a\}=g(7,a), \forall a$.

Special Functions

- Theorem 5.4:
  Let $f : A \times A \to B$ be a binary operation. If f has an identity, then that identity is unique.
  - **Proof** If f has more than one identity, let $x_1, x_2 \in A$

    $f(a, x_1) = a = f(x_1, a), \forall a \in A$

    $f(a, x_2) = a = f(x_2, a), \forall a \in A$

    For x_1 is identity $\Rightarrow f(x_1, x_2) = x_2$

    For x_2 is identity $\Rightarrow f(x_1, x_2) = x_1$

    $\therefore x_1 = x_2$

Special Functions

- **Ex 5.35:** If A={x, a, b, c, d}, how many closed binary operations on A have x as the identity?

Table 5.2

f	x	a	b	c	d
x	x	a	b	c	d
a	a	—	—	—	—
b	b	—	—	—	—
c	c	—	—	—	—
d	d	—	—	—	—

Let f: A x A→A with f(x, y)=y=f(y, x) for all y∈A

5^{16} closed binary operations on A where x is the identity

Of these $5^{10} = 5^{4} * 5^{(4*4-4)/2}$ are commutative.

對角　上三角

5^{17} closed binary operations on A that have an identity

Of these 5^{11} are commutative

(5^16)*5 { x, a, b, c, d } = 5^17

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 （只map到R+)

- 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), $D \subseteq A_1 \times A_2 \times A_3 \times A_4$

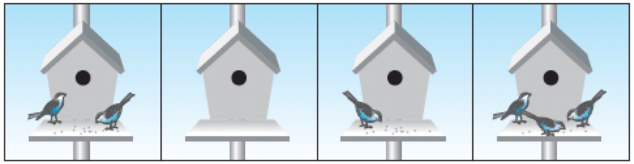
Course Number	Course Title	Professor	Section Letter
MA 111	Calculus I	P. Z. Chinn	A
MA 111	Calculus I	V. Larney	B
MA 112	Calculus II	J. Kinney	A
MA 113	Calculus III	A. Schmidt	A

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



5.5 The Pigeonhole Principle

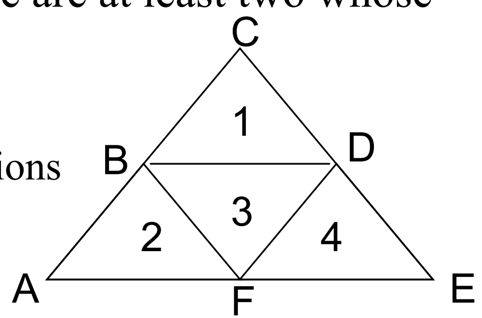
- The pigeonhole principle: If m pigeons occupy n pigeonholes and $m > n$, then at least one pigeonhole has two or more pigeons roosting in it.
  - Proof by contradiction: if the result is not true, then each pigeonhole has at most one pigeon roosting in it, so a total of at most n ($< m$) pigeons.
- **Ex 5.39** : An office employs 13 clerks, so at least two of them must have birthdays during the same month.
- **Ex 5.41** : Wilma operates a computer with a magnetic tape drive. One day she is given a tape that contains 500,000 "word" of four or fewer lowercase letters. Can it be that the 500,000 words are all distinct?
  - **Solution**

$$26^4 + 26^3 + 26^2 + 26 = 475{,}254$$

$$\therefore \text{at least one word is repeated on the tape.}$$

The Pigeonhole Principle

- **Ex 5.42** : Let $S \subset \mathbf{Z}^+$, where $|S| = 37$. Then S contains two elements that have the same remainder upon division by 36.
  - **Hint** $n = 36q + r,\ 0 \le r < 36.$
- **Ex 5.44** : Any subset of size 6 from the set S = {1,2,3,…,9} must contain two elements whose sum is 10.
  - **Hint** $\{1,9\},\{2,8\},\{3,7\},\{4,6\},\{5\}$. ***Pigeon? Pigenhole?***
- **Ex 5.45** : Triangle ACE is equilateral with $AC = 1$. If five points are selected from the interior of the triangle, there are at least two whose distance apart is less than ½.
  - ***Related with Pigeonhole principle ?***
  - **Hint** Break up the interior of ACE into 4 regions



Ex 5.46 Let S be a set of six (*distinct*) positive integers whose maximum is at most 14. Show that the sums of the elements in all the nonempty subsets of S cannot all be distinct.

For any nonempty subset A of S, the sum of the elements in A, denoted S_A, satisfies

$1 \le S_A \le 9 + 10 + \cdots + 14 = 69$, and there are

$2^6 - 1 = 63$ nonempty subsets of S. (too many pigeonholes!)

選or不選 - 全不沒選

Consider the subset of less than 6 elements.

pigeonholes=10+11+...+14=**60**

pigeons=2^6-1-1=**62**=63-1 (only S have 6 elements)

VIP pigeon!

The Pigeonhole Principle

- Ex 5.47 : Let $m \in \mathbf{Z}^+$ with m odd. Prove that there exists a positive integer n such that m divides 2^n - 1
  - **Proof**

除m會有兩數有相同餘數

Consider the $m+1$ positive integers $2^1-1, 2^2-1, \cdots, 2^m-1, 2^{m+1}-1$,

By the pigeonhole principle, exists $s, t \in \mathbf{Z}^+$, with $1 \le s < t \le m+1$,

where 2^s-1 and 2^t-1 have the same remainder upon division by m

$\therefore 2^s-1 = q_1 m + r$ and $2^t-1 = q_2 m + r \Rightarrow 2^t - 2^s = (q_2-q_1)m$

$\because 2^t - 2^s = 2^s(2^{t-s}-1)$ and m is odd $\therefore \gcd(2^s, m) = 1$

$\therefore m \mid 2^{t-s}-1$

Ex 5.48 28 days to play at most 40 sets of tennis and at least 1 play per day. Prove there is a consecutive span of days during which exactly 15 sets are played.

在28天中至多打40場球，每天至少打一場。

証明必存在有連續數天所打的球賽總和為剛好15場。

當為連續的，假設其總共次數的變數

For $1 \le i \le 28$, let x_i be the total number of sets played from the start to the end of i-th day. Then $1 \le x_1 < x_2 < \mathrm{L} < x_{28} \le 40$, $x_1 + 15 < x_2 + 15 < \mathrm{L} < x_{28} + 15 \le 40 + 15 = 55$. Of the 56 integers, since their maximum is 55, two of them must be the same. Hence there exist $1 \le j < i \le 28$ with $x_i = x_j + 15$. From day $j+1$ to the end of day i, exactly 15 sets are played.

The Pigeonhole Principle

- **Ex 5.49** : For each $n \in \mathbf{Z}^+$, a sequence of $n^2 + 1$ **distinct** real numbers contains a decreasing or increasing subsequence of $n + 1$.
  - **Example**
    1. The sequence 6, 5, 8, 3, 7 (length 5, n=2) contains the decreasing subsequence 6, 5, 3 (length 3)
    2. The sequence 11, 8, 7, 1, 9, 6, 5, 10, 3, 12 (length 10, n=3) contains the increasing subsequence 8, 9, 10, 12 (length 4)
  - **Proof**

    Let $a_1, a_2, \cdots, a_{n^2+1}$ be a sequence of n^2+1 distinct real numbers, $1 \le k \le n^2+1$

    x_k = the maximum length of a decreasing subsequence that ends with a_k

    y_k = the maximum length of a increasing subsequence that ends with a_k

k	1	2	3	4	5	6	7	8	9	10
a_k	11	8	7	1	9	6	5	10	3	12
x_k	1	2	3	4	2	4	5	2	6	1
y_k	1	1	1	1	2	2	2	3	2	4

Prove one of x_k or $y_k \ge n+1$

相異的 pair

The Pigeonhole Principle

- **Proof**

If no descreasing or increasing subsequence of length $n+1$, then $1 \le x_k \le n, 1 \le y_k \le n$.

$\therefore$ at most n^2 distinct pairs (x_k, y_k)

But, we have n^2+1 pairs (a sequence of n^2+1 distinct real numbers)

$\Rightarrow$ two identical pairs $(x_i, y_i), (x_j, y_j), i \ne j$, let $i < j$ (pigeonhole principle)

In fact, if $a_i < a_j$ then $y_i < y_j$; while if $a_j < a_i$ then $x_j > x_i$.

$\Rightarrow$ two pairs $(x_i, y_i) \ne (x_j, y_j)$

This contradiction tells us that $x_k = n+1$ or $y_k = n+1$ for some $n+1 \le k \le n^2+1$.

n^2+1

k	1	2	3	4	5	6	7	8	9	10
a_k	11	8	7	1	9	6	5	10	3	12
x_k	1	2	3	4	2	4	5	2	6	1
y_k	1	1	1	1	2	2	2	3	2	4

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 $a \in \mathrm{A}$
- Definition 5.17:
  $f, \mathrm{g} : A \to B$, 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

- 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

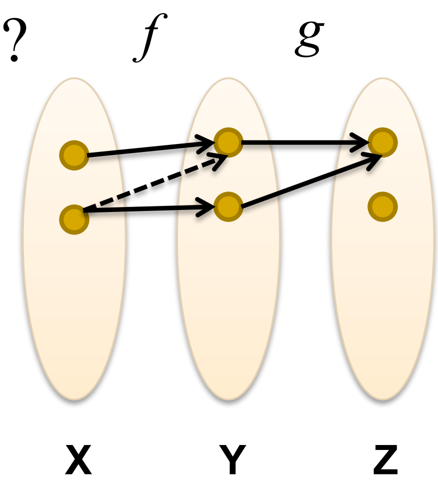
- Theorem 5.5:

$$\text{Let } f: A \to B \text{ and } g: B \to C.$$
$$\text{a) If } f \text{ and } g \text{ are one-to-one, then } g \circ f \text{ is one-to-one.}$$
$$\text{b) If } f \text{ and } g \text{ are onto, then } g \circ f \text{ is onto.}$$

  - Proof

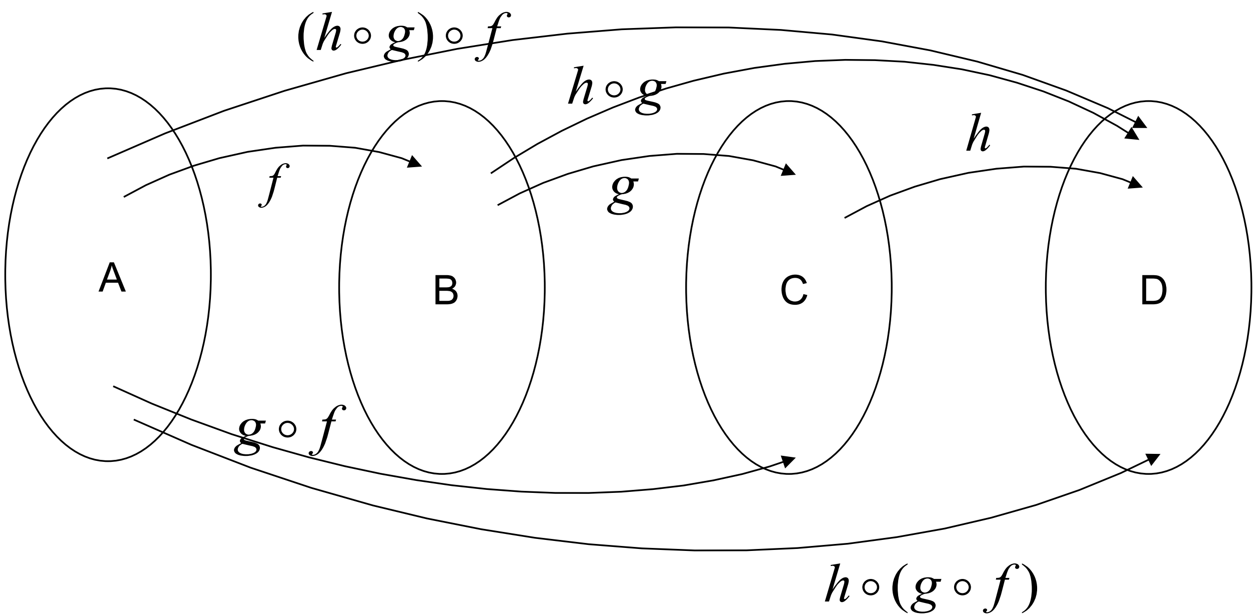
$$\text{a) Let } a_1, a_2 \in A \text{ with } (g \circ f)(a_1) = (g \circ f)(a_2)$$
$$\Rightarrow g(f(a_1)) = g(f(a_2)) \Rightarrow f(a_1) = f(a_2) (\because g \text{ is one-to-one})$$
$$\Rightarrow a_1 = a_2 (\because f \text{ is one-to-one})$$
$$\therefore g \circ f \text{ is one-to-one}$$
$$\text{b)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

- Let f: $X \rightarrow Y$ and g: $Y \rightarrow Z$ be functions. Which statement is **FALSE**?
  - T If $g \circ f$ is one-to-one, f is one-to-one?
  - F If $g \circ f$ is one-to-one, g is one-to-one?
  - T If $g \circ f$ is onto, g is onto?
  - T If $g \circ f$ is bijection, g is onto?
  - T If $g \circ f$ is bijection, f is one-to-one?



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** :
  $4 \to 3 \to 1 \to 2$
  $A = \{1,2,3,4\}$, $f: A \to A$, and $f = \{(1,2),(2,2),(3,1),(4,3)\}$
  $f^2 = f \circ f = \{(1,2),(2,2),(3,2),(4,1)\}$, $f^3 = f \circ f^2 = \{(1,2),(2,2),(3,2),(4,2)\}$
  長度為2的路徑
  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** :
  $A = \{1,2,3\}$, $B = \{\mathrm{w,x,y}\}$, $f: A \to B$, and $f = \{(1,w),(2,x),(3,y)\}$
  $\Rightarrow f^c = \{(w,1),(x,2),(y,3)\} \Rightarrow f^c \circ f = 1_A$, $f \circ f^c = 1_B$
  identity function

Function Composition and Inverse Functions

- Definition 5.21:
  If $f : A \to B$, then f is said to be <u>invertible</u>, if there is function $g : B \to A$, such that $g \circ f = 1_A$ and $f \circ g = 1_B$. 反函式
- <u>**Ex 5.58**</u> : 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: $f : A \rightarrow B$ is invertible $\Leftrightarrow$ it is one-to-one and onto.
  - **Proof**

    (1) Assuming that $f : A \rightarrow B$ is invertible, and exists unique $g : B \rightarrow A$ 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 $b \in B \Rightarrow g(b) \in A$

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

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

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

    define $g : B \rightarrow A$ 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, $f^{-1}(x) = \ln x$

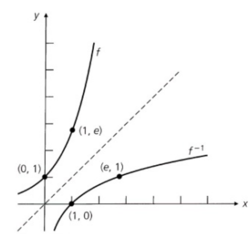


Figure 5.10

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

- **Ex 5.63** : $f : \mathbf{R} \to \mathbf{R}$ is defined by $f(x) = \begin{cases} 3x - 5, x > 0 \\ -3x + 1, x \le 0 \end{cases}$

  What is $f^{-1}([-5,5])$?

  - **Solution**

$$f^{-1}([-5,5]) = \{x \mid f(x) \in [-5,5]\} = \{x \mid -5 \le f(x) \le 5\}$$

(i) $x > 0$: $\quad -5 \le 3x - 5 \le 5$

$0 \le 3x \le 10$

$0 \le x \le 10/3, \therefore 0 < x \le 10/3$

(ii) $x \le 0$: $\quad -5 \le -3x + 1 \le 5$

$-6 \le -3x \le 4$

$-4/3 \le x \le 2, \therefore -4/3 \le x \le 0$

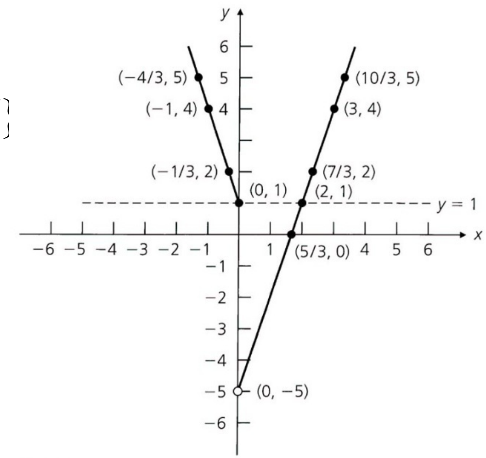


Figure 5.11

$$\therefore f^{-1}([-5,5]) = \{x \mid -4/3 \le x \le 0 \text{ or } 0 < x \le 10/3\} = [-4/3,\ 10/3]$$

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) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$ (c) $f^{-1}(\overline{B_1}) = \overline{f^{-1}(B_1)}$.
  - **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

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

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

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

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

m Objects Are Distinct	n Containers Are Distinct	Some Container(s) May Be Empty	Number of Distributions
Yes	Yes	Yes	n^m
Yes	Yes	No	$n!\,S(m, n)$ (#onto function)
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 $|f(n)| \leq m|g(n)|$ for all $n \in \mathbf{Z}^+$, where $n \geq k$.

  - "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) $1 \leq n \leq 4 : f(1) = 5, g(1) = 1; f(2) = 10, g(2) = 4; f(3) = 15,$

  $g(3) = 9$; $f(4) = 20, g(4) = 16$

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

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

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

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

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

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 $\varepsilon=0$

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)

Smart Algorithms

- Sorting n elements: not $\Omega(n^2)$ but $\Theta(n \log n)$

- Multiplying two n-bit numbers, not $\Omega(n^2)$, not $\Omega(n^{1.58\ldots})$, but $O(n \log n \log \log n)$, and maybe even faster

- Matrix multiplication: not $\Omega(n^3)$, but $O(n^{2.41\ldots})$, generally believed to be $O(n^2)$.

- …

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

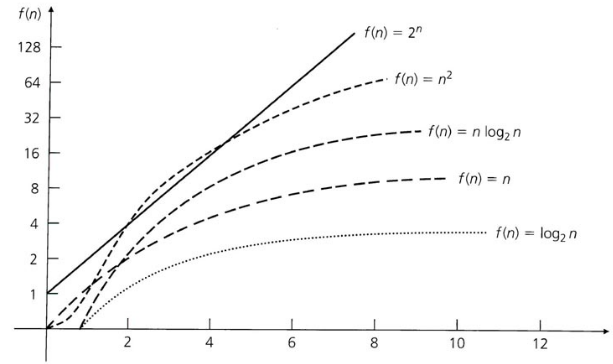


Figure 5.17

- 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	$1.84*10^{19}$	$>10^{89}$

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