Department of Computer Science
National Tsing Hua University

CS 2336: Discrete Mathematics

Chapter 5

Relations and Functions

Instructor: Cheng-Hsin Hsu

Outline

Cartesian Products

- Definition 5.1: For sets A, B the Cartesian product, or cross product, of A and B is denoted by $A \times B$ and equals $\{(a, b) | a \in A, b \in B\}$
  - (a,b) is called an ordered pair
  - (a,b)=(c,d) iff ?
  - $|A \times B| = |A||B| = |B \times A|$
  - $A \times B = B \times A?$
- Extension: For sets $A_1, A_2, \ldots, A_n$, their product is denoted as $A_1 \times A_2 \times \cdots \times A_n$, and is equal $\{(a_1, a_2, \ldots, a_n) | a_i \in A_i, 1 \leq i \leq n\}$

Examples 5.1, 5.2, 5.3

- Ex 5.1: Let $A=\{2, 3, 4\}$, $B=\{4,5\}$. Derive (i) $A \times B$, (ii) $B \times A$, (iii) B^2, (iv) B^3.

- Ex 5.2: What are (i) $\mathbb{R} \times \mathbb{R}$,(ii) $\mathbb{R}^+ \times \mathbb{R}^+$; and (iii) $\mathbb{R}^3$?

- Ex 5.3: Let $C=\{x,y\}$, draw tree diagrams for (i) $A \times B$ (ii) $B \times A$, and (iii) $A \times B \times C$. Show the size of each of the Cartesian product.

Binary Relation

- Consider sets A, B, any subset of $A \times B$ is called a (binary) relation from A to B. Any subset of A^2 is called a (binary) relation on A.
- Ex 5.5: $A=\{2, 3, 4\}$, $B=\{4,5\}$, give a few samples of relations. How many relations in total from A to B?
- Formally: For two sets $|A|=m$ and $|B|=n$, there are 2^{mn} relations from A to B, including the empty set and $A \times B$. For a relation $\mathscr{R}_1$ from A to B, we can construct a relation $\mathscr{R}_2$ from B to A. (but how?)

Examples 5.6, 5.7, and 5.8

- Ex 5.6: Let $B=\{1,2\}$, and $A = \mathscr{P}(B)$, give an example of a relation on A. Give an example of subset relation.

- Ex 5.7: Define a relation $\mathscr{R}$ on $\mathbb{Z}^+$ as $\{(x,y)|x \leq y\}$. Can we write down all the pairs in it?

- Ex 5.8: $\mathscr{R} = \{(m,n)|n = 7m\}$ is a subset of $\mathbb{N} \times \mathbb{N}$. Define $\mathscr{R}$ recursively. Then show $(3,21)$ is in $\mathscr{R}$.

Some Observations

- For any set A, $A \times \emptyset = \emptyset$. Why?

- $A \times (B \cap C) = (A \times B) \cap (A \times C)$
- $A \times (B \cup C) = (A \times B) \cup (A \times C)$
- $(B \cap C) \times A = (B \times A) \cap (C \times A)$
- $(B \cup C) \times A = (B \times A) \cup (C \times A)$

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

Function

- For nonempty set A, B, a function, or mapping, f from A to B, denoted as $f : A \rightarrow B$, is a relation from A to B. Every element of A appears exactly once in the relation.
  - (a,b) is an order pair of function f, we write $f(a)=b$
  - b is the image of a under f, and a is a preimage of b
  - each $a \in A$, there is a unique $f(a)$ in B
  - $(a,b),(a,c)$ in f implies $b=c$

Example 5.9

- For $A=\{1,2,3\}$, $B=\{w,x,y,z\}$
  - Is $\{(1,w),(2,x),(3,x)\}$ a function? a relation?
  - Is $\{(1,w),(2,x)\}$ a function? a relation?
  - Is $\{(1,w),(2,w),(2,x),(3,z)\}$ a function? a relation?

Domain and Codomain

- For $f : A \rightarrow B$, A is the domain of f and B is the codomain of f. The subset of B that contains all the second components of pairs of f is range of f, denoted by $f(A)$.
  - The range of f is the images of A under f.

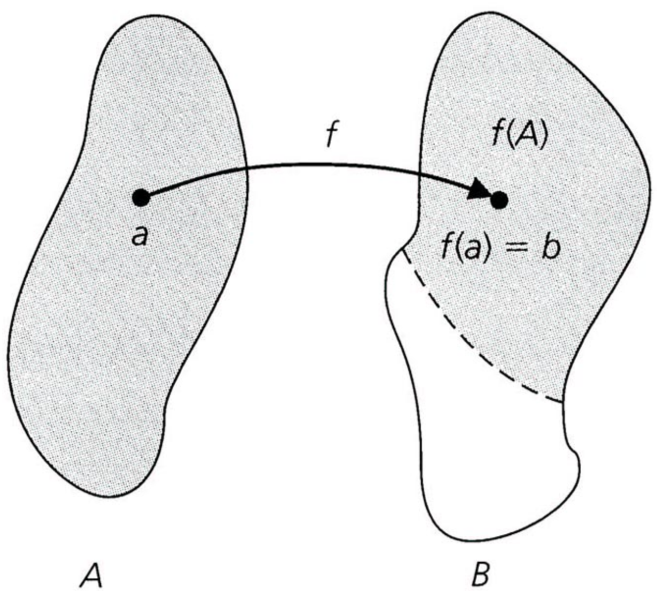

Figure 5.4

Examples 5.10 and 5.12

- Ex 5.10: Several interesting functions
  - Floor function $f: \mathbf{R} \to \mathbf{Z},\ f(x) = \lfloor x \rfloor$
  - Ceiling function $g: \mathbf{R} \to \mathbf{Z},\ g(x) = \lceil x \rceil$
  - Truncation function ? $t: \mathbf{R} \to \mathbf{Z}$
  - Row-major implementation to store 2-dim array into a 1-min array. For $A = (a_{ij})_{m \times n}$, let $f(a_{ij})$ be the offset of element a_{ij}. $f(a_{ij})=(i-1)n+j$.
- Ex 5.12: A sequence of real number can be seen as a function $f: \mathbb{Z}^+ \to \mathbb{R}$

Number of Functions

- Consider Ex 5.9: For $A=\{1,2,3\}$, $B=\{w,x,y,z\}$
  - How many relations in total from A to B?
  - How many functions in total from A to B?

- Formally: For two sets $|A|=m$ and $|B|=n$, there are $n^m=|B|^{|A|}$ functions from A to B. Why?
  - Different from relation, the number of functions from A to B is generally different from that from B to A

One-to-One Function

- Definition 5.5: A function $f: A \to B$ is called one-to-one, or injective, if each element of *B* appears at at most once as the image of an element of *A*
  - What do we know about |*A*| and |*B*|
  - *f* is one-to-one iff for all a_1, a_2 in *A*, $f(a_1)=f(a_2)$ implies $a_1=a_2$
- Ex 5.13: Prove or disprove: (i) $f: \mathbb{R} \to \mathbb{R}, f(x) = 3x + 7$ and (ii) $g: \mathbb{R} \to \mathbb{R}, g(x) = x^4 - x$ are one-to-one functions
- Ex 5.14: A={1,2,3} and B={1,2,3,4,5} How about *f*={(*1*,*1*),(*2*,*3*),(*3*,*4*)} and *g*={(*1*,*2*),(*2*,*3*),(*3*,*2*)}?

Number of 1-1 Functions

- Consider Ex 5.9: For $A=\{1,2,3\}$, $B=\{w,x,y,z\}$
  - How many relations in total from A to B?
  - How many functions in total from A to B?
  - How many one-to-one functions in total from A to B?
- Formally: For two sets $|A|=m$ and $|B|=n$, there are $P(n,m)$ one-to-one functions from A to B. Why?

Image

- For $f: A \to B, A_1 \subseteq A$, $f(A_1) = \{b \in B | b = f(a), a \in A_1\}$ is called the image of A_1 under f.

- Ex 5.15: $f=\{(1,w),(2,x),(3,x),(4,y),(5,y)\}$. Give the images of $\{1\},\{1,2\},\{1,2,3\},\{2,3\},\{2,3,4,5\}$.
- Ex 5.16: (a) $g: \mathbb{R} \to \mathbb{R}, g(x) = x^2$ What are (i) $g(R)$, (ii) $g(Z)$, and (iii) $g([-2, 1])$?
- Ex 5.16: (b) $h: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, h(x, y) = 2x + 3y$, (i) prove the range of $h(.)$ is Z and (ii) what is $h(0,z)$, where z in Z?

Images of Subsets

- Theorem 5.2 Let $f : A \to B$, where $A_1, A_2 \subseteq A$, prove
  - $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$
  - $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$
  - $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ when f is $1 - 1$

Restriction and Extension

- If $f : A \to B, A_1 \subseteq A$, then $f|_{A_1} : A_1 \to B$ is the restriction of f to A_1 if $f|_{A_1}(a) = f(a)\ \forall a \in A_1$
- If $A_1 \subseteq A, f : A_1 \to B$, then g is the extension of f to A if $g : A \to B, g(a) = f(a)\ \forall\ a \in A_1$

Examples 5.17 and 5.18

- Ex 5.17: $A=\{1,2,3,4,5\}$
  - $f : A \to \mathbb{R}, f = \{(1,10),(2,13),(3,16),(4,19),(5,22)\}$
  - $g : \mathbb{Q} \to \mathbb{R}, g(q) = 3q + 7, \ \forall\ q \in \mathbb{Q}$
  - $h : \mathbb{R} \to \mathbb{R}, h(r) = 3r + 7, \ \forall\ r \in \mathbb{R}$
  - Show the restrictions/extension relations among them
- Ex 5.18: Let $f : A \to B, g : A_1 \to B$, where $g = f|_{A_1}$
  - f is an extension of g from A_1 to A
  - How many ways to extend g from A_1 to A?

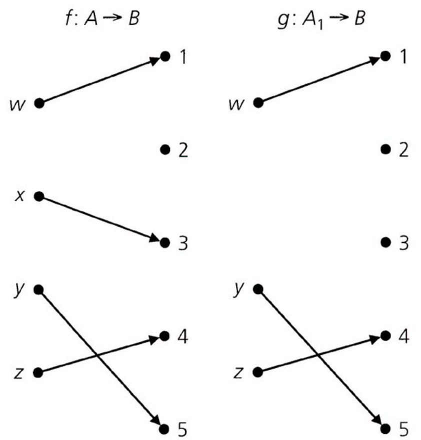

Figure 5.5

Outline

Onto Function

- A function $f : A \to B$ is called onto, or subjective, if $f(A)=B$. In other words, for all $b \in B$ there is at least one $a \in A$ with $f(a)=b$.
  - Only exist when $|A| >= |B|$
- Ex 5.19: Are the following functions onto?
  (i) $f : \mathbb{R} \to \mathbb{R}, f(x) = x^3$, (ii) $g : \mathbb{R} \to \mathbb{R}, g(x) = x^2$, and
  (iii) $h : \mathbb{R} \to [0, \infty), h(x) = x^2$; what are the ranges?
- Ex 5.20: Is $f(x)=3x+1$ an onto function from Z to Z? How about (i) from Q to Q, and (ii) from R to R? Are they one-to-one functions?

Number of Onto Functions

- Ex 5.22: Let $A=\{x,y,z\}$, B=$\{1,2\}$, consider $f : A \to B$
  - How many functions are not onto?
  - How many functions are onto?
  - In fact, if $|A|=m>=2$ and $|B|=2$, there are 2^m-2 onto functions. What happens if $m=1$?
- Ex 5.23: Let $A=\{w,x,y,z\}$, $B=\{1,2,3\}$, how many onto functions from A to B?
  - Number of functions from A to B?
  - Number of functions from A to $\{1,3\}$? And $\{1\}$?
  - In fact, if $|A|=m>=3$ and $|B|=3$, there are $C(3,3)3^m-C(3,2)2^m+C(3,1)1^m$ onto functions.

Principle of Inclusion and Exclusion

- For $|A|=m$, $|B|=n$, there are

$$C(n,n)n^m - C(n,n-1)(n-1)^m + \cdots + (-1)^{n-1}C(n,1)1^m$$
$$= \sum_{k=0}^{n-1}(-1)^k C(n,n-k)(n-k)^m$$ onto functions from A to B

- Ex 5.24: $A=\{1,2,3,4,5,6,7\}$, $B=\{w,x,y,z\}$. How many onto functions from A to B?

Examples 5.25

- Ex 5.25: There are four assistants, including Teresa, who will be responsible for seven bank accounts. Assume Teresa is responsible for the most valuable account, how many ways can the accounts be assigned to the assistants so that each of them works on at least one account?
  - What if Teresa only work on the most valuable account?
  - What if Teresa also work on other accounts?

Examples 5.26

- Ex 5.26: There are *36* onto functions from $A=\{a,b,c,d\}$ to $B=\{1,2,3\}$. Here, we consider the containers in *B* are distinguishable.
  - What if the containers are identical?
  - For example, $\{a,b\}_1$; $\{c\}_2$;$\{d\}_3$ is the same as $\{c\}_1$;$\{a,b\}_2$,$\{d\}_3$

Stirling Number of the 2nd Kind

- For *m*>=*n*, there are $\sum_{k=0}^{n}(-1)^k C(n,n-k)(n-k)^m$ ways to distribute *m* objects to *n* numbered containers without any empty container
- Make the containers into identical, the number of ways for object distribution becomes
$$\frac{1}{n!}\sum_{k=0}^{n}(-1)^k C(n,n-k)(n-k)^m$$
- This is called the Stirling number of the second kind, and written as $S(m,n)$
  - There are $n!S(m,n)$ onto functions from A to B

Sample Stirling Numbers

Table 5.1

m \ n	1	2	3	4	5	6	7	8
	$S(m, n)$							
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

Theorem 5.3

- Let m, n be positive number, $1<n<=m$, we have $S(m+1,n)=S(m,n-1)+nS(m,n)$

- Ex 5.28: Consider $30030 = 2 \times 3 \times 5 \times 7 \times 11 \times 13$, how many unordered factorizations of this number?
  - How many ways to factorize this number into two containers?
  - How about three containers?

Outline

Binary and Unary Operations

- A function $f : A \times A \rightarrow B$ is called a binary operation on A. If $B \subseteq A$, then the binary operation is closed on A or closed under f.
- A function $g : A \rightarrow A$ is called a unary operation on A
- Ex 5.29: (a) Is $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, f(a, b) = a - b$ a closed binary operation? (b) Is $g : \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \mathbb{Z}, f(a, b) = a - b$ closed?

Commutative and Associative

- Let $f : A \times A \rightarrow B$
  - If $f(a, b)=f(b,a)$ for all $(a, b) \in A \times A$, f is commutative
  - When $B \subseteq A$, if $f(f(a,b),c)=f(a,f(b,c))$ for all $a, b, c \in A$, f is called associative

- Ex 5.32: (a) Is $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, f(a, b) = a + b - 3ab$ (i) commutative and (ii) associative? (b) How about $h : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, h(a, b) = a|b|$?

- Ex. 5.33: Let $A= \{a,b,c,d\}$. How many binary operations on A? How many commutative closed binary operations on A?

Identify

- Let $f : A \times A \to B$ be a binary operation on A. An element $x \in A$ is called an identify for *f* if *f*(*a*,*x*)=*f*(*x*,*a*)=*a*, for all *a*.

- What is the identify:
  - $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, f(a, b) = a + b$
  - $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, f(a, b) = a - b$
  - $A = \{1, 2, 3, 4, 5, 6\}, f : \mathbb{A} \times \mathbb{A} \to \mathbb{A}, f(a, b) = \min\{a, b\}$

Uniqueness of Identify

- Let $f : A \times A \to B$ be a binary operation. If f has an identify, then the identify is unique.

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

Projection

- If $D \subseteq A \times B$, then $\pi_A : D \to A, \pi_A(a,b) = a$ is called the projection on the first coordinate. Similarly, we can define π_B.
  - If $D = A \times B$, then π_A and π_B are both onto.

- Ex 5.36: Let $A=\{w,x,y\}$, $B=\{1,2,3,4\}$, $D=\{(x,1),(x,2),(x,3),(y,1),\{y,4)\}$. What are $\pi_A(D)$ and $\pi_B(D)$? Are they onto?
- Ex 5.37: Let $A = B = \mathbb{R}, D \subseteq A \times B, D = \{(x,y)|y = x^2\}$ Determine $\pi_A(D)$ and $\pi_B(D)$.

Extended Projection

- Let $A_1, A_2, \ldots, A_n$ be sets, $\{i_1, i_2, \ldots, i_m\} \subseteq \{1, 2, \ldots, n\}$ where $i_1 < i_2 < \cdots < i_m$ and $m \leq n$. If $D \subseteq \times_{i=1}^{n} A_i$, then the function $\pi : D \to A_{i_1} \times A_{i_2} \times \cdots \times A_{i_m}$, with $\pi(a_1, a_2, \ldots, a_n) = (a_{i_1}, a_{i_2}, \ldots, a_{i_m})$ is the projection of D on $i_1, i_2, \ldots, i_m$ coordinates.
- Ex 5.38: $D \subseteq A_1 \times A_2 \times A_3 \times A_4$

Table 5.3

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 112	Calculus II	A. Schmidt	B
MA 112	Calculus II	R. Mines	C
MA 113	Calculus III	J. Kinney	A

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

Pigeonhole Principle

- If *m* pigeons occupy *n* pigeonholes and $m>n$, then at least one pigeonhole has two or more pigeons in it

- Ex 5.39: An office employs 13 clerks, at least two of them must have birthdays in the same month.
- Ex 5.40: Larry has 12 pairs of socks in a laundry bag. Drawing the socks from the bag randomly, he will have to draw at most 13 of them to get a matched pair.

More Pigeonhole Examples

- Ex 5.41: There are 500,000 words with four or fewer lowercase letters. Can all the words be distinct?
- Ex 5.42: Let $S \subset \mathbb{Z}^+$, where $|S|=37$. Then S contains two elements that have the same remainder upon division by 36.
- Ex 5.44: Any subset of size 6 from $S=\{1,2,3,\ldots,9\}$ must contain two elements whose sum is 10.

Outline

Bijective and Identify Function

- If $f : A \to B$, then f is bijective, or be a one-to-one correspondence, if it is both one-to-one and onto.

- Ex 5.50: If $A=\{1,2,3,4\}$ and $B=\{w,x,y,z\}$, then $f=\{(1,w),(2,x),(3,y),(4,z)\}$ is a one-to-one correspondence from A to B.

- $1_A : A \to A, 1_A(a) = a \ \forall \ a \in A$ is called the identify function for A

Equal Function

- $f, g : A \to B$, if $f(a)$=$g(a)$ for all a, then we say f and g are equal and write f=g

- Ex 5.51: Let $f : \mathbb{Z} \to \mathbb{Z}, g : \mathbb{Z} \to \mathbb{Q}$, where $f(x) = x = g(x)$ for all $x \in \mathbb{Z}$. Are they equal? If not, why?

- Ex 5.52: Show that $f, g : \mathbb{R} \to \mathbb{Z}$, where $g(x) = \lceil x \rceil$ and $f(x) = x$ if $x \in \mathbb{Z}$; $f(x) \lfloor x \rfloor + 1$ if $x \in \mathbb{R} - \mathbb{Z}$, are they equal?

Composite Function

- If $f : A \to B$ and $g : B \to C$, the composite function is defined as $g \circ f : A \to C, (g \circ f)(a) = g(f(a)), \forall a \in A$

- Ex 5.53: $f=\{(1,a),(2,a),(3,b),(4,c)\}$, $g=\{(a,x),(b,y),(c,z)\}$, give $g(f(x))$.

- Ex 5.54: $f, g : \mathbb{R} \to \mathbb{R}$, where $f(x)=x^2$, $g(x)=x+5$. Show that $(g \circ f)(x) \neq (f \circ g)(x)$

Theorems 5.5 and 5.6

- Let $f : A \to B$ and $g : B \to C$
  - If f and g are one to one, then $g \circ f$ is one to one
  - If f and g are onto, then $g \circ f$ is onto
- If $f : A \to B, g : B \to C, h : C \to D$, then

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

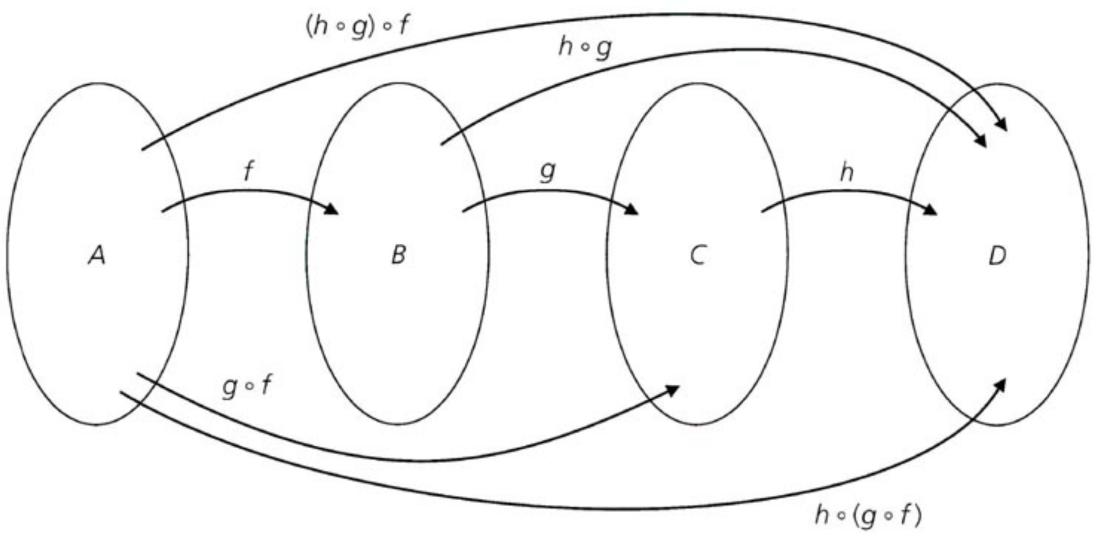

Figure 5.9

Powers of Functions

- If $f : A \to A$, we define $f^1 = f$ and $f^{n+1} = f \circ (f^n)$
- Ex 5.56: Let $A=\{1,2,3,4\}$, and a function $f=\{(1,2), (2,2),(3,1),(4,3)\}$. What are f^2, f^3, f^4?

Converse and Invertible Function

- If $\mathscr{R}$ is a relation from A to B. The converse of $\mathscr{R}$, written as $\mathscr{R}^c$, is given as $\mathscr{R}^c = \{(b,a) | (a,b) \in \mathscr{R}\}$
- Ex 5.57: $A=\{1,2,3\}$ and $B=\{w,x,y\}$. Let $f=\{(1,w), (2,x),(3,y)\}$, write f^c. What is $f^c \circ f$?

- If $f : A \rightarrow B$ then function f is invertible if there is a function g such that $g \circ f = 1_a, f \circ g = 1_B$
- Ex 5.58: Let $f, g : \mathbb{R} \rightarrow \mathbb{R}$ are defined as $f(x)=2x+5$, $g(x)=(1/2)(x-5)$ Show that f and g are both invertible.

Uniqueness of Invert Function

- If a function $f : A \to B$ is invertible, there is a function $g : B \to A$ satisfies $g \circ f = 1_A, f \circ g = 1_B$, then *g* is unique

- Theorem: A function is invertible if and only if it is one-to-one and onto.

- Ex 5.59: $f_1 : \mathbb{R} \to \mathbb{R}, f_1(x) = x^2$ and

  $f_2 : [0, \infty) \to [0, \infty), f_2(x) = x^2$.

  Are they invertible?

Theorem 5.9

- If $f: A \to B, g: B \to C$ are invertible, then $g \circ f: A \to C$ is invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

- Ex 5.60: Let $m, b \in \mathbb{R}, m \neq 0$, is the function $f: \mathbb{R} \to \mathbb{R}$ where $f = \{(x, y) | y = mx + b\}$ invertible? What is f^{-1}?

- Ex 5.61: Let $f: \mathbb{R} \to \mathbb{R}^+, f(x) = e^x$. Give $f^{-1}(x)$.

Preimage

- If $f : A \to B, B_1 \subseteq B$, then $f^{-1}(B_1) = \{x \in A | f(x) \in B_1\}$. The set $f^{-1}(B_1)$ is called the preimage of B_1 under f.
- Ex 5.62: Let $A=\{1,2,3,4,5,6\}$, $B=\{6,7,8,9,10\}$. If $f=\{(1,7),(2,7),(3,8),(4,6),(5,9),(6,9)\}$. Consider $B_1=\{6,8\}$, $B_2=\{7,8\}$, $B_3=\{3,5,6\}$, $B_4=\{8,9,10\}$, $B_5=\{8,10\}$. Compute the preimages of these subsets.
- Ex 5.64: $f : \mathbb{Z} \to \mathbb{R}, f(x) = x^2 + 5$ and $g : \mathbb{R} \to \mathbb{R}, g(x) = x^2 + 5$

Table 5.9

B	$f^{-1}(B)$
$\{6\}$	$\{-1, 1\}$
$[6, 7]$	$\{-1, 1\}$
$[6, 10]$	$\{-2, -1, 1, 2\}$
$[-4, 5)$	$\emptyset$
$[-4, 5]$	$\{0\}$
$[5, +\infty)$	$\mathbf{Z}$

Table 5.10

B	$g^{-1}(B)$
$\{6\}$	$\{-1, 1\}$
$[6, 7]$	$[-\sqrt{2}, -1] \cup [1, \sqrt{2}]$
$[6, 10]$	$[-\sqrt{5}, -1] \cup [1, \sqrt{5}]$
$[-4, 5)$	$\emptyset$
$[-4, 5]$	$\{0\}$
$[5, +\infty)$	$\mathbf{R}$

Theorems 5.10 and 5.11

- If $f : A \rightarrow B$, and $B_1, B_2 \subseteq B$
  - $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$
  - $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$
  - $f^{-1}(\overline{B_1}) = \overline{f^{-1}(B_1)}$

- Let $f : A \rightarrow B, |A| = |B|$. The following statements are equivalent: (i) *f* is one-to-one, (ii) *f* is onto, and (iii) *f* is invertible.

Note

The remaining two sections will be discussed between Chapters 9 and 10

Outline

Algorithm

- Properties of general algorithms
  - Step-by-step instructions
  - Takes inputs and generates outputs
  - Solves certain class of problems (not a single instance)
  - Uniqueness of results based on the input (mostly)
  - Terminates after a finite number of instructions
- What else are we looking for?
  - How fast an algorithm runs? (efficiency)
  - How good are the resulting solutions? (optimality)

Efficiency

- Example: If we like to compute a^n for $a \in \mathbb{R}, n \in \mathbf{Z}^+$ is there a function of n that can describe how fast the algorithm accomplishes it?
  - n represents the size of the problem
  - We are looking for a time-complexity function $f(n)$
  - In general, $f(n)$ increases when n increases, and we care about $f(n)$ with larger n more

Domination

- Let $f, g : \mathbb{Z}^+ \to \mathbb{R}$, we say that *g* dominates *f* of there exist $m \in \mathbb{R}^+, k \in \mathbb{Z}^+$ such that $|f(n)| \leqslant m|g(n)|$ for all $n \in \mathbb{Z}^+$, where $n \geqslant k$.

- When *f* is dominated by *g*, we say that *f* is of order (at most) *g*, and we write $f \in O(g)$, which is read as order *g* or big-O of *g*
  - *O*(*g*) represents all the functions that are dominated by *g*

- Ex 5.65: $f(n)=5n$, $g(n)=n^2$, show that *g* dominates *f*
  - Are the choices of *m* and *k* unique?

Observations

- Domination is not unique, e.g., a function dominated by $O(n)$ will be dominated by $O(n^2)$ as well!
- Consider $f, g, h : \mathbb{Z}^+ \to \mathbb{R}$, where $f \in O(g)$ and $g \in O(h)$.
  - We know $f \in O(h)$
  - However, unless $h \in O(g)$, we know $O(g)$ is a tighter bound than $O(h)$, and we prefer to say $f \in O(g)$, which provides more information

Big-O Classes

Table 5.11

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
$O(n^m)$, $m = 0, 1, 2, 3, \ldots$	Polynomial
$O(c^n)$, $c > 1$	Exponential
$O(n!)$	Factorial

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

Complexity Analysis

- Below is a subroutine computing the account balance after *n* months, where *n* is a positive integer. Let *f*(*n*) denote the number of operations, which big-O class is *f*(*n*) in?

```
procedure AccountBalance(n: integer)
begin
   deposit := 50.00        {The monthly deposit}
   i := 1                  {Initializes the counter}
   rate := 0.005           {The monthly interest rate}
   balance := 100.00       {Initializes the balance}
   while i ≤ n do
      begin
         balance := deposit + balance + balance * rate
         i := i + 1
      end
end
```

Figure 5.12

Best-, Average-, and Worst-Case

- Consider the problem of searching a key k from a list of n numbers, $a_1, a_2, a_3, \ldots, a_n$. Function f represents the number of comparisons a searching algorithm takes.
  - What are the complexities of f in the best-, average-, and worst-cases?

```
procedure LinearSearch(key, n: integer; a1,a2,a3,...,an: integers)
begin
  i := 1                          {initializes the counter}
  while (i ≤ n and key ≠ ai) do
    i := i + 1
  if i ≤ n then location := i     {successful search}
  else location := 0              {unsuccessful search}
end {location is the subscript of the first array entry that equals key;
    location is 0 if key is not found}
```

Figure 5.13

Which Algorithm is More Efficient?

- Consider two functions to compute a^n, where a is a real number and n is a positive integer

```
procedure Power1(a: real; n: positive integer)
begin
   x := 1.0
   for i := 1 to n do
      x := x * a
end
```

Figure 5.14

Which Algorithm is More Efficient? (cont.)

- Consider two functions to compute a^n, where a is a real number and n is a positive integer

```
procedure Power2(a: real; n: positive integer)
begin
   x := 1.0
   i := n
   while i > 0 do
     begin
       if i ≠ 2 * ⌊i/2⌋ then     {i is odd}
          x := x * a
       i := ⌊i/2⌋
       if i > 0 then
          a := a * a
     end
end
```

Figure 5.15

Which Algorithm is More Efficient? (cont.)

- Consider two functions to compute a^n, where a is a real number and n is a positive integer

```
n = 7
x := 1.0
i := 7

   x := x * a     {x = a}
1  i := 3
   a := a * a

   x := x * a     {x = a^3}
2  i := 1
   a := a * a

3  x := x * a     {x = a^7}
   i := 0

   [x = a^7 = a · a^2 · a^4]
```

```
n = 8
x := 1.0
i := 8

1  i := 4
   a := a * a

2  i := 2
   a := a * a

3  i := 1
   a := a * a

4  x := x * a     {x = a^8}
   i := 0

   [x = (((a)^2)^2)^2]
```

Figure 5.16

Limitations of Big-O Notations

- Even though $f(n) \in O(n), g(n) \in O(n^2)$, $f(n)$ is not always more efficient than $g(n)$
  - Consider $f(n) = 1000n$ and $g(n) = n^2$

- We can only say $f(n)$ is likely more efficient than $g(n)$ when n is large enough
  - Thus, Big-O notations make more sense when n is large

Limitations of Big-O Notations (cont.)

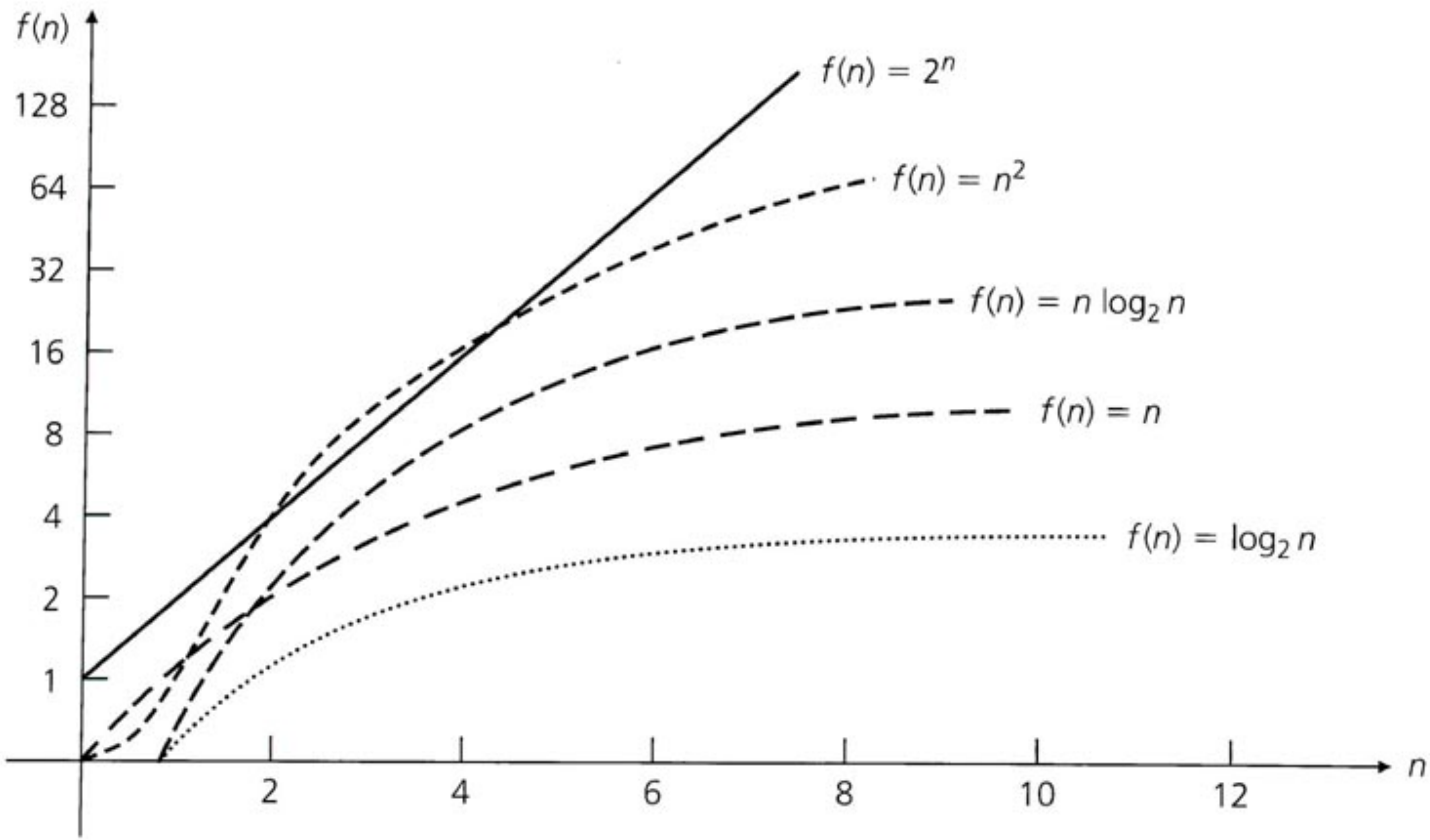

Figure 5.17

Take-home Exercises

- Exercise 5.1: 1, 3, 6, 8, 12
- Exercise 5.2: 4, 8, 15, 20, 27
- Exercise 5.3: 1, 4, 8, 12, 16
- Exercise 5.4: 1, 2, 5, 8, 12
- Exercise 5.5: 2, 6, 13, 14, 20
- Exercise 5.6: 7, 10, 16, 17, 22