



# CS201H DISCRETE MATHEMATICS FOR COMPUTER SCIENCE

Dr. QI WANG

Department of Computer Science and Engineering

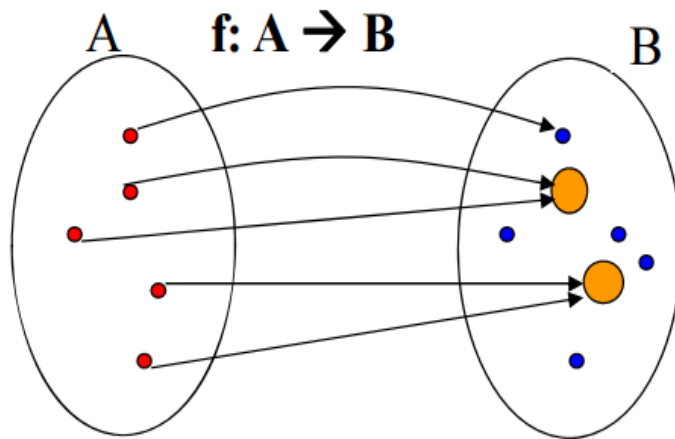
Office: Room413, CoE South Tower

Email: [wangqi@sustech.edu.cn](mailto:wangqi@sustech.edu.cn)

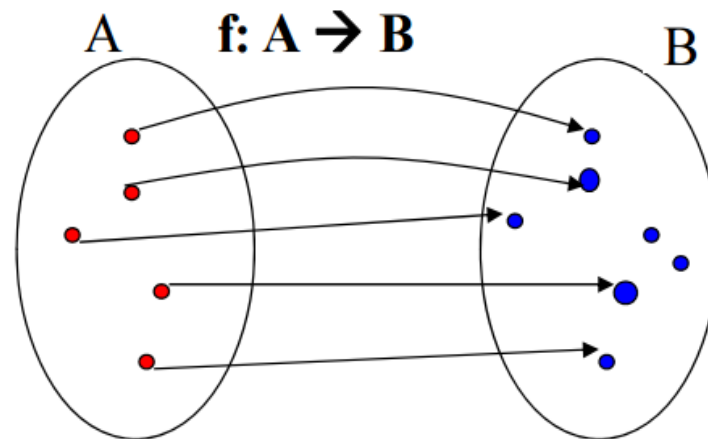
# Injective (One-to-One) Function

- A function  $f$  is called *one-to-one* or *injective*, if and only if  $f(x) = f(y)$  implies  $x = y$  for all  $x, y$  in the domain of  $f$ . In this case,  $f$  is called an *injection*.

Alternatively: A function is *one-to-one* if and only if  $f(x) \neq f(y)$  whenever  $x \neq y$ . (contrapositive!)



**Not injective**



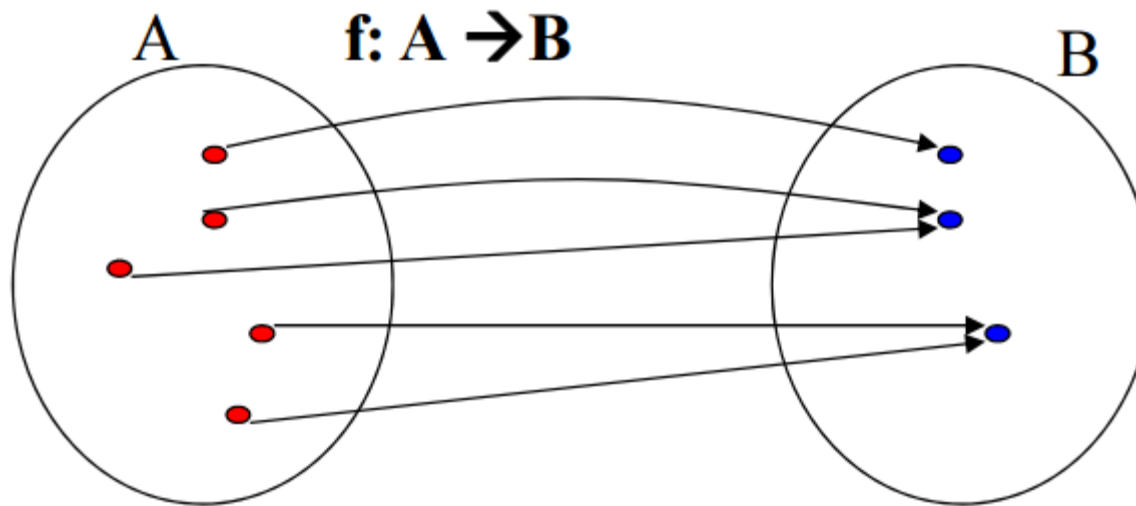
**Injective function**



# Surjective (Onto) Function

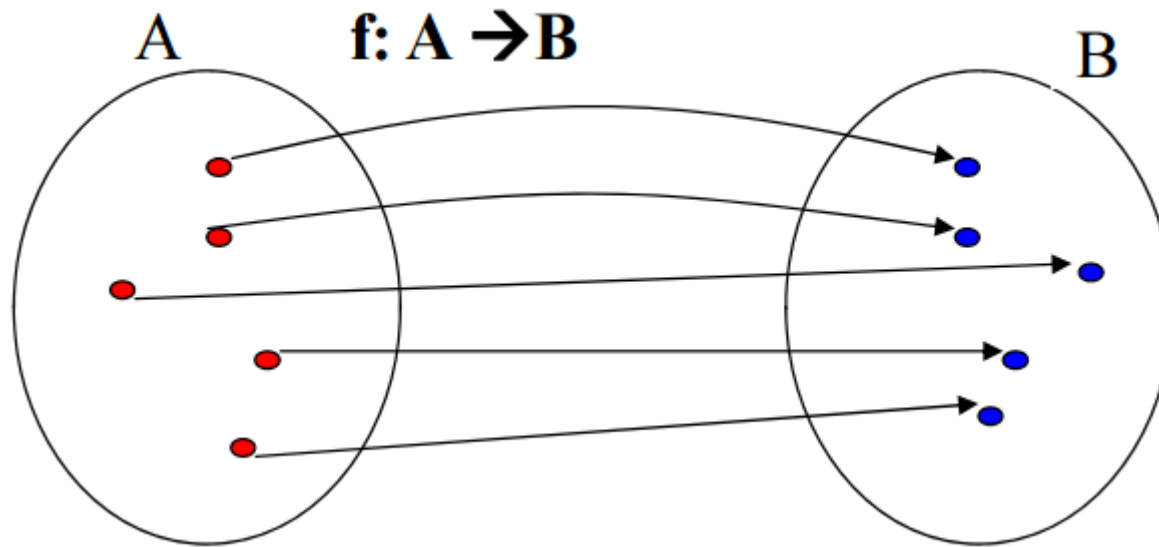
- A function  $f$  is called *onto* or *surjective*, if and only if for every  $b \in B$  there is an element  $a \in A$  such that  $f(a) = b$ . In this case,  $f$  is called a *surjection*.

Alternatively: A function is *onto* if and only if **all** codomain elements are covered ( $f(A) = B$ ).



# Bijjective Function (One-to-One Correspondence)

- A function  $f$  is called *bijjective*, if and only if it is both one-to-one and onto.



# Bijjective Functions

- “For a function  $f : A \rightarrow B$  with  $|A| = |B| = n$ ,  $f$  is one-to-one if and only if  $f$  is onto.”



# Bijjective Functions

- “For a function  $f : A \rightarrow B$  with  $|A| = |B| = n$ ,  $f$  is one-to-one if and only if  $f$  is onto.”
- “For a function  $f$  from  $A$  to itself,  $f$  is one-to-one if and only if  $f$  is onto, where  $A$  is infinite.”



# Bijjective Functions

- “For a function  $f : A \rightarrow B$  with  $|A| = |B| = n$ ,  $f$  is one-to-one if and only if  $f$  is onto.”
- “For a function  $f$  from  $A$  to itself,  $f$  is one-to-one if and only if  $f$  is onto, where  $A$  is infinite.”

## Counterexample:

$f : \mathbf{Z} \rightarrow \mathbf{Z}$ , where  $f(x) = 2x$ .

$f$  is one-to-one but not onto

- $1 \mapsto 2$
- $2 \mapsto 4$
- $3 \mapsto 6$

3 has no preimage.



# Composition of Functions

- Suppose that  $f$  is a bijection from  $A$  to  $B$ . Then  $f \circ f^{-1} = I_B$  and  $f^{-1} \circ f = I_A$ , Since

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a$$

$$(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b,$$

where  $I_A, I_B$  denote the *identity functions* on the sets  $A$  and  $B$ , respectively.





# Some Important Functions

- The *floor function* assigns a real number  $x$  the **largest** integer that is  $\leq x$ , denoted by  $\lfloor x \rfloor$ .
- The *ceiling function* assigns a real number  $x$  the **smallest** integer that is  $\geq x$ , denoted by  $\lceil x \rceil$ .



# Some Important Functions

- The *floor function* assigns a real number  $x$  the **largest** integer that is  $\leq x$ , denoted by  $\lfloor x \rfloor$ .
- The *ceiling function* assigns a real number  $x$  the **smallest** integer that is  $\geq x$ , denoted by  $\lceil x \rceil$ .

**TABLE 1** Useful Properties of the Floor and Ceiling Functions.

( $n$  is an integer,  $x$  is a real number)

(1a)  $\lfloor x \rfloor = n$  if and only if  $n \leq x < n + 1$

(1b)  $\lceil x \rceil = n$  if and only if  $n - 1 < x \leq n$

(1c)  $\lfloor x \rfloor = n$  if and only if  $x - 1 < n \leq x$

(1d)  $\lceil x \rceil = n$  if and only if  $x \leq n < x + 1$

(2)  $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$

(3a)  $\lfloor -x \rfloor = -\lceil x \rceil$

(3b)  $\lceil -x \rceil = -\lfloor x \rfloor$

(4a)  $\lfloor x + n \rfloor = \lfloor x \rfloor + n$

(4b)  $\lceil x + n \rceil = \lceil x \rceil + n$



# Some Important Functions

Ex. 1: Prove or disprove that if  $x$  is a real number, then  $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$ .

Ex. 2: Prove or disprove that  $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$  for all real numbers  $x$  and  $y$ .



# Some Important Functions

Ex. 1: Prove or disprove that if  $x$  is a real number, then  $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$ .

Ex. 2: Prove or disprove that  $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$  for all real numbers  $x$  and  $y$ .

- The **factorial function**  $f : \mathbf{N} \rightarrow \mathbf{Z}^+$  is the product of the first  $n$  positive integers when  $n$  is a nonnegative integer, denoted by  $f(n) = n!$ .



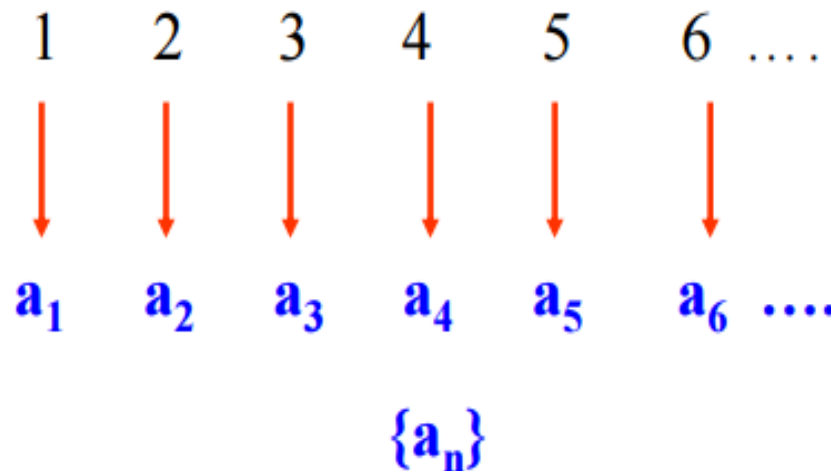
# Sequences

- A *sequence* is a function from a subset of the set of integers (typically the set  $\{0, 1, 2, \dots\}$  or  $\{1, 2, 3, \dots\}$  to a set  $S$ . We use the notation  $a_n$  to denote the image of the integer  $n$ . ( $\{a_n\}$  represents the ordered list  $a_1, a_2, a_3, \dots$ )



# Sequences

- A *sequence* is a function from a subset of the set of integers (typically the set  $\{0, 1, 2, \dots\}$  or  $\{1, 2, 3, \dots\}$  to a set  $S$ . We use the notation  $a_n$  to denote the image of the integer  $n$ . ( $\{a_n\}$  represents the ordered list  $a_1, a_2, a_3, \dots$ )



## 1.1 Basic Concepts and Notation

In general, a *sequence* is an ordered list of elements from a set  $S$ . Formally, a *finite sequence* with elements over  $S$  is a function from the index set  $\{0, 1, \dots, N-1\}$  to  $S$  for some integer  $N \geq 0$ , and  $N$  is called the *length* of the sequence. An *infinite sequence* with elements over  $S$  is a function from the integer group  $\mathbf{Z}$  to  $S$ , and a *semi-infinite sequence* with elements over  $S$  is a function from the semi-group  $\{0, 1, \dots\}$  to  $S$ . If the set  $S$  is a finite field  $\mathbb{F}_q$  with  $q$  elements, we say that the sequence is a  $q$ -ary sequence over  $\mathbb{F}_q$ . In particular, if  $S = \text{GF}(2)$ , the sequence is called a *binary sequence*.

For a sequence  $\mathbf{s} = (s_i)_{i \geq 0}$ , if there exist integers  $r > 0$  and  $u \geq 0$  such that

$$s_{i+r} = s_i \quad \text{for all } i \geq u, \quad (1.1)$$

the sequence is said to be *ultimately periodic* with parameters  $(r, u)$ , and  $r$  is called a *period* of the sequence  $\mathbf{s}$ . The smallest number  $r$  satisfying (1.1) is called the *least period*



# Sequences

## ■ Examples:

- ◇  $a_n = n^2$ , where  $n = 1, 2, 3, \dots$
- ◇  $a_n = (-1)^n$ , where  $n = 0, 1, 2, \dots$
- ◇  $a_n = 2^n$ , where  $n = 0, 1, 2, \dots$





# Sequences

## ■ Examples:

- ◇  $a_n = n^2$ , where  $n = 1, 2, 3, \dots$
- ◇  $a_n = (-1)^n$ , where  $n = 0, 1, 2, \dots$
- ◇  $a_n = 2^n$ , where  $n = 0, 1, 2, \dots$

- An *arithmetic progression* is a sequence of the form  $a, a + d, a + 2d, a + 3d, \dots, a + nd, \dots$ , where the *initial term*  $a$  and *common difference*  $d$  are real numbers.



# Sequences

## ■ Examples:

- ◇  $a_n = n^2$ , where  $n = 1, 2, 3, \dots$
- ◇  $a_n = (-1)^n$ , where  $n = 0, 1, 2, \dots$
- ◇  $a_n = 2^n$ , where  $n = 0, 1, 2, \dots$

- An *arithmetic progression* is a sequence of the form  $a, a + d, a + 2d, a + 3d, \dots, a + nd, \dots$ , where the *initial term*  $a$  and *common difference*  $d$  are real numbers.

## Example:

- ◇  $a_n = -1 + 4n$ , where  $n = 0, 1, 2, 3, \dots$



# Geometric Progression

- A **geometric progression** is a sequence of the form  $a, ar, ar^2, \dots, ar^n, \dots$ , where the *initial term*  $a$  and the *common ratio*  $r$  are real numbers.



# Geometric Progression

- A **geometric progression** is a sequence of the form  $a, ar, ar^2, \dots, ar^n, \dots$ , where the *initial term*  $a$  and the *common ratio*  $r$  are real numbers.

## Example:

◇  $a_n = (1/2)^n$ , where  $n = 0, 1, 2, 3, \dots$



# Geometric Progression

- A **geometric progression** is a sequence of the form  $a, ar, ar^2, \dots, ar^n, \dots$ , where the *initial term*  $a$  and the *common ratio*  $r$  are real numbers.

## Example:

◇  $a_n = (1/2)^n$ , where  $n = 0, 1, 2, 3, \dots$

## Question:

Given a sequence, **how to find a rule for generating the sequence?**



# Geometric Progression

- A **geometric progression** is a sequence of the form  $a, ar, ar^2, \dots, ar^n, \dots$ , where the *initial term*  $a$  and the *common ratio*  $r$  are real numbers.

## Example:

◇  $a_n = (1/2)^n$ , where  $n = 0, 1, 2, 3, \dots$

## Question:

Given a sequence, **how to find a rule for generating the sequence?**

8, 42, 226, 1232, 6646, 35362, 185868, ...



# Recursively Defined Sequences

- The  $n$ -th element of the sequence  $\{a_n\}$  is defined recursively in terms of the previous elements of the sequence and the initial elements of the sequence.



# Recursively Defined Sequences

- The  $n$ -th element of the sequence  $\{a_n\}$  is defined recursively in terms of **the previous elements** of the sequence and **the initial elements of the sequence**.

## Examples:

- ◇  $a_n = a_{n-1} + 2$  assuming  $a_0 = 1$ , for  $n \geq 1$
- ◇  $f_n = f_{n-1} + f_{n-2}$  for  $n = 2, 3, 4, \dots$  (*Fibonacci sequence*)





# Summations

- The *summation of the terms of a sequence* is

$$\sum_{j=m}^n a_j = a_m + a_{m+1} + \cdots + a_n$$

The variable  $j$  is referred to as *the index of summation* and the choice of the letter  $j$  is *arbitrary*.

- ◇  $m$  is the *lower limit*
- ◇  $n$  is the *upper limit* of the summation



# Summations

- The *summation of the terms of a sequence* is

$$\sum_{j=m}^n a_j = a_m + a_{m+1} + \cdots + a_n$$

The variable  $j$  is referred to as *the index of summation* and the choice of the letter  $j$  is *arbitrary*.

- ◇  $m$  is the *lower limit*
- ◇  $n$  is the *upper limit* of the summation

$$\sum_{j=1}^n (ax_j + by_j) = a \sum_{j=1}^n x_j + b \sum_{j=1}^n y_j$$

$$\sum_{i=1}^m \sum_{j=1}^n a_i b_j = \sum_{i=1}^m a_i \sum_{j=1}^n b_j$$



# Summations

- The sum of the first  $n$  terms of the arithmetic progression  $a, a + d, a + 2d, \dots, a + nd$  is

$$S = \sum_{j=0}^n (a + jd) = (n + 1)a + d \sum_{j=0}^n j = (n + 1)a + d \frac{n(n + 1)}{2}$$

- The sum of the first  $n$  terms of the geometric progression  $a, ar, ar^2, \dots, ar^n$  is

$$S = \sum_{j=0}^n (ar^j) = a \sum_{j=0}^n r^j = a \frac{r^{n+1} - 1}{r - 1}$$



# Examples

## ■ Examples:

$$\diamond S = \sum_{j=1}^5 (2 + 3j)$$

$$\diamond S = \sum_{j=3}^5 (2 + 3j)$$

$$\diamond S = \sum_{i=1}^4 \sum_{j=1}^2 (2i - j)$$

$$\diamond S = \sum_{j=0}^3 2(5)^j$$

$$\diamond S = \sum_{i=1}^4 \sum_{j=1}^3 ij$$



# Examples

## ■ Examples:

$$\diamond S = \sum_{j=1}^5 (2 + 3j) \quad 55$$

$$\diamond S = \sum_{j=3}^5 (2 + 3j) \quad 42$$

$$\diamond S = \sum_{i=1}^4 \sum_{j=1}^2 (2i - j) \quad 28$$

$$\diamond S = \sum_{j=0}^3 2(5)^j \quad 312$$

$$\diamond S = \sum_{i=1}^4 \sum_{j=1}^3 ij \quad 60$$



# Infinite Series

- Infinite geometric series can be computed in the closed form for  $|x| < 1$ .



# Infinite Series

- Infinite geometric series can be computed in the closed form for  $|x| < 1$ .

$$\sum_{k=0}^{\infty} x^k = \lim_{n \rightarrow \infty} \sum_{k=0}^n x^k = \lim_{n \rightarrow \infty} \frac{x^{n+1} - 1}{x - 1} = \frac{1}{1 - x}$$



# Infinite Series

- Infinite geometric series can be computed in the closed form for  $|x| < 1$ .

$$\sum_{k=0}^{\infty} x^k = \lim_{n \rightarrow \infty} \sum_{k=0}^n x^k = \lim_{n \rightarrow \infty} \frac{x^{n+1} - 1}{x - 1} = \frac{1}{1 - x}$$

$$\sum_{k=0}^{\infty} kx^{k-1} = \frac{1}{(1 - x)^2}$$





# Some Useful Summation Formulas

**TABLE 2** Some Useful Summation Formulae.

<i>Sum</i>	<i>Closed Form</i>
$\sum_{k=0}^n ar^k \ (r \neq 0)$	$\frac{ar^{n+1} - a}{r - 1}, r \neq 1$
$\sum_{k=1}^n k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^n k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^n k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=0}^{\infty} x^k,  x  < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{\infty} kx^{k-1},  x  < 1$	$\frac{1}{(1-x)^2}$



# Cardinality of Sets

- Recall: the cardinality of a finite set is defined by the number of the elements in the set.



# Cardinality of Sets

- Recall: the cardinality of a finite set is defined by the number of the elements in the set.
- The sets  $A$  and  $B$  have *the same cardinality* if there is a one-to-one correspondence between elements in  $A$  and  $B$ .



# Cardinality of Sets

- Recall: the cardinality of a finite set is defined by the number of the elements in the set.
- The sets  $A$  and  $B$  have *the same cardinality* if there is a one-to-one correspondence between elements in  $A$  and  $B$ .
- If there is a one-to-one function from  $A$  to  $B$ , the cardinality of  $A$  is less than or the same as the cardinality of  $B$ , denoted by  $|A| \leq |B|$ . Moreover, when  $|A| \leq |B|$  and  $A$  and  $B$  have different cardinalities, we say that the cardinality of  $A$  is less than the cardinality of  $B$ , denoted by  $|A| < |B|$ .



# Countable Sets

- A set that is **either finite** or **has the same cardinality as the set of positive integers  $\mathbb{Z}^+$**  is called *countable*.  
A set that is **not countable** is called *uncountable*.



# Countable Sets

- A set that is **either finite** or **has the same cardinality as the set of positive integers  $\mathbb{Z}^+$**  is called *countable*. A set that is **not countable** is called *uncountable*.

Why are these called **countable**?



# Countable Sets

- A set that is **either finite** or **has the same cardinality as the set of positive integers  $\mathbb{Z}^+$**  is called *countable*. A set that is **not countable** is called *uncountable*.

Why are these called **countable**?

- ◇ The elements of the set can be **enumerated and listed**.



# Hilbert's Grand Hotel

- The Grand Hotel has **countably infinite number of rooms**, each occupied by a guest. We can always accommodate a new guest at this hotel. How is this possible?





# Hilbert's Grand Hotel

- The Grand Hotel has **countably infinite number of rooms**, each occupied by a guest. We can always accommodate a new guest at this hotel. How is this possible?

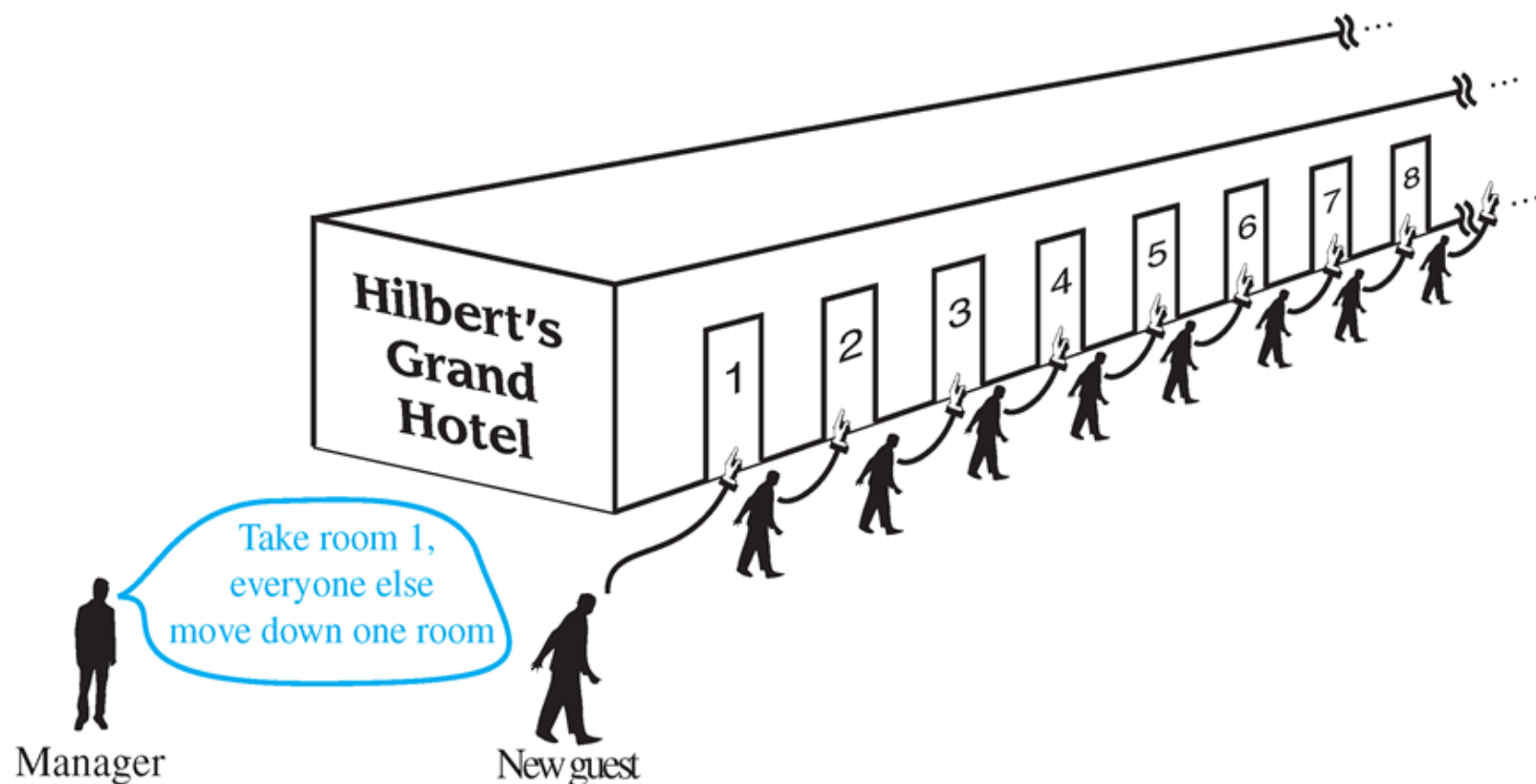


FIGURE 2 A New Guest Arrives at Hilbert's Grand Hotel.

# Countable Sets

## ■ Example 1

$A = \{0, 2, 4, 6, \dots\}$  – set of even numbers. Is it countable?



# Countable Sets

## ■ Example 1

$A = \{0, 2, 4, 6, \dots\}$  – set of even numbers. Is it countable?

Using the **definition**: Is there a **bijection**  $f : \mathbf{Z}^+ \rightarrow A$ ?



# Countable Sets

## ■ Example 1

$A = \{0, 2, 4, 6, \dots\}$  – set of even numbers. Is it countable?

Using the **definition**: Is there a **bijection**  $f : \mathbf{Z}^+ \rightarrow A$ ?

Define a function  $f : x \mapsto 2x - 2$ . This is a bijection!

**one-to-one** Why?

**onto** Why?



# Countable Sets

## ■ Example 1

$A = \{0, 2, 4, 6, \dots\}$  – set of even numbers. Is it countable?

Using the **definition**: Is there a **bijection**  $f : \mathbf{Z}^+ \rightarrow A$ ?

Define a function  $f : x \mapsto 2x - 2$ . This is a bijection!

**one-to-one** Why?

if  $2x - 2 = 2y - 2$ , then  $x = y$

**onto** Why?

$\forall x \in A$ ,  $(x + 2)/2$  is the preimage in  $\mathbf{Z}^+$



# Countable Sets

- **Example 2 (Theorem)**

The set of integers  $\mathbb{Z}$  is countable.



# Countable Sets

## ■ Example 2 (Theorem)

The set of integers  $\mathbf{Z}$  is countable.

### Solution:

We can list a sequence:

$$0, 1, -1, 2, -2, 3, -3, \dots$$

or define a **bijection** from  $\mathbf{Z}^+$  to  $\mathbf{Z}$ :

- when  $n$  is even:  $f(n) = n/2$
- when  $n$  is odd:  $f(n) = -(n-1)/2$



# Countable Sets

## ■ Example 3 (Theorem)

The set of (positive) rational numbers is countable.





# Countable Sets

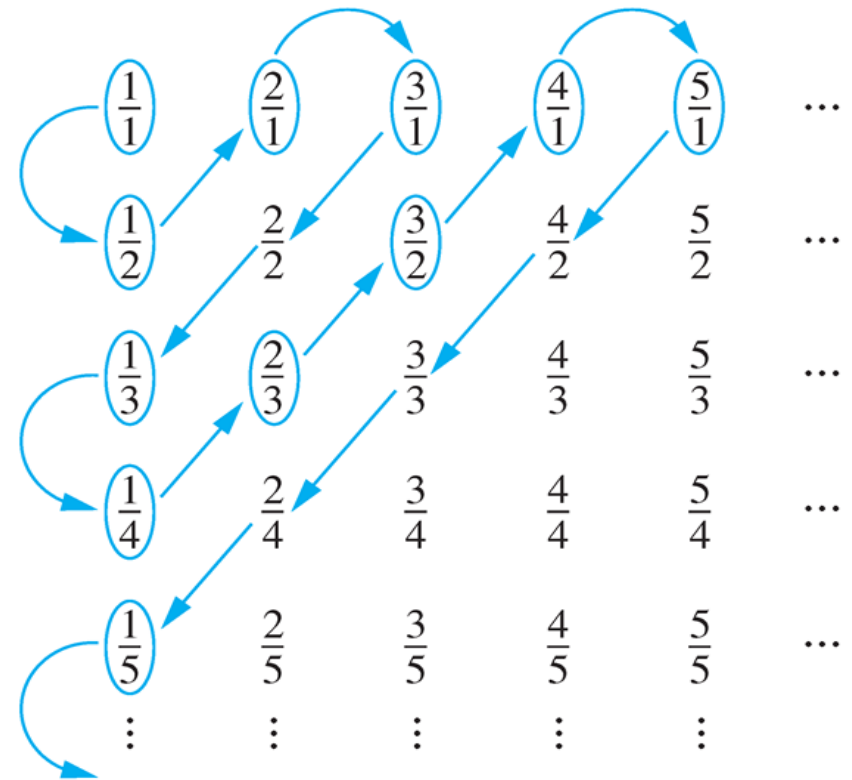
## ■ Example 3 (Theorem)

The set of (positive) rational numbers is countable.

### Solution:

Constructing the list: first list  $p/q$  with  $p + q = 2$ , next list  $p/q$  with  $p + q = 3$ , and so on.

$1, 1/2, 2, 3, 1/3, 1/4, 2/3, \dots$



# Countable Sets

## ■ Example 4 (Theorem)

The set of finite strings  $S$  over a finite alphabet  $A$  is countably infinite. (Assume an alphabetical ordering of symbols in  $A$ )



# Countable Sets

## ■ Example 4 (Theorem)

The set of finite strings  $S$  over a finite alphabet  $A$  is countably infinite. (Assume an alphabetical ordering of symbols in  $A$ )

### Solution:

We show that the strings can be listed in a sequence. First list

- (i) all the strings of length 0 in alphabetical order.
- (ii) then all the strings of length 1 in lexicographic order.
- (iii) and so on.

This implies a bijection from  $\mathbb{Z}^+$  to  $S$ .



# Countable Sets

## ■ Example 5

The set of all Java programs is countable.



# Countable Sets

## ■ Example 5

The set of all Java programs is countable.

### Solution:

Let  $S$  be the set of strings constructed from the characters which may appear in a Java program. Use the ordering from the previous example. Take each string in turn

- feed the string into a Java compiler
- if the compiler says YES, this is a syntactically correct Java program, we add this program to the list
- we move on to the next string

In this way, we construct a bijection from  $\mathbb{Z}^+$  to the set of Java programs.



# Uncountable Sets

## ■ Theorem

The set of real numbers  $\mathbf{R}$  is uncountable.



# Uncountable Sets

## ■ Theorem

The set of real numbers  $\mathbf{R}$  is uncountable.

### Proof by contradiction:

Assume that  $\mathbf{R}$  is countable. Then every subset of  $\mathbf{R}$  is countable (why?), in particular, the interval from 0 to 1 is countable. This implies that the elements of this set can be listed as  $r_1, r_2, r_3, \dots$ , where

$$- r_1 = 0.d_{11}d_{12}d_{13}d_{14}\cdots$$

$$- r_2 = 0.d_{21}d_{22}d_{23}d_{24}\cdots$$

$$- r_3 = 0.d_{31}d_{32}d_{33}d_{34}\cdots$$

$$\text{all } d_{ij} \in \{0, 1, 2, \dots, 9\}.$$



# Uncountable Sets

## ■ Theorem

The set of real numbers  $\mathbf{R}$  is uncountable.

### Proof by contradiction:

We want to show that not all real numbers in the interval between 0 and 1 are in this list.

Form a new number called  $r = 0.d_1d_2d_3d_4 \cdots$ , where  $d_i = 2$  if  $d_{ii} \neq 2$ , and  $d_i = 3$  if  $d_{ii} = 2$ .





# Uncountable Sets

## ■ Theorem

The set of real numbers  $\mathbf{R}$  is uncountable.

### Proof by contradiction:

We want to show that not all real numbers in the interval between 0 and 1 are in this list.

Form a new number called  $r = 0.d_1d_2d_3d_4 \cdots$ , where  $d_i = 2$  if  $d_{ii} \neq 2$ , and  $d_i = 3$  if  $d_{ii} = 2$ .

Example: suppose	$r_1 = 0.\textcolor{red}{7}5243\dots$	$d_1 = 2$
	$r_2 = 0.5\textcolor{red}{2}4310\dots$	$d_2 = 3$
	$r_3 = 0.13\textcolor{red}{1}257\dots$	$d_3 = 2$
	$r_4 = 0.936\textcolor{red}{3}633\dots$	$d_4 = 2$
	$\dots$	$\dots$
	$r_t = 0.23222\textcolor{red}{2}22\dots$	$d_t = 3$



# Uncountable Sets

## ■ Theorem

The set of real numbers  $\mathbf{R}$  is uncountable.

### Proof by contradiction:

We claim that  $r$  is different from each number in the list.

Each expansion is unique, if we exclude an infinite string of 9's.  $r$  and  $r_i$  differ in the  $i$ -th decimal place for all  $i$ .



# Uncountable Sets

## ■ Theorem

The set of real numbers  $\mathbf{R}$  is uncountable.

### Proof by contradiction:

We claim that  $r$  is different from each number in the list.

Each expansion is unique, if we exclude an infinite string of 9's.  $r$  and  $r_i$  differ in the  $i$ -th decimal place for all  $i$ .

This is called *Cantor diagonalization argument*.



# Uncountable Sets

## ■ Theorem

The set  $\mathcal{P}(\mathbb{N})$  is uncountable.

# Uncountable Sets

## ■ Theorem

The set  $\mathcal{P}(\mathbb{N})$  is uncountable.

### Proof by contradiction:

Assume that  $\mathcal{P}(\mathbb{N})$  is countable. This implies that the elements of this set can be listed as  $S_0, S_1, S_2, \dots$ , where  $S_i \subseteq \mathbb{N}$ , and each  $S_i$  can be represented uniquely by the bit string  $b_{i0}b_{i1}b_{i2}\dots$ , where  $b_{ij} = 1$  if  $j \in S_i$  and  $b_{ij} = 0$  if  $j \notin S_i$

$$- S_0 = b_{00}b_{01}b_{02}b_{03}\dots$$

$$- S_1 = b_{10}b_{11}b_{12}b_{13}\dots$$

$$- S_2 = b_{20}b_{21}b_{22}b_{23}\dots$$

$$\vdots$$

$$\text{all } b_{ij} \in \{0, 1\}.$$

# Uncountable Sets

## ■ Theorem

The set  $\mathcal{P}(\mathbb{N})$  is uncountable.

### Proof by contradiction:

Form a new set called  $R = b_0b_1b_2b_3 \cdots$ , where  $b_i = 0$  if  $b_{ii} = 1$ , and  $b_i = 1$  if  $b_{ii} = 0$ .

# Uncountable Sets

## ■ Theorem

The set  $\mathcal{P}(\mathbb{N})$  is uncountable.

### Proof by contradiction:

Form a new set called  $R = b_0b_1b_2b_3 \dots$ , where  $b_i = 0$  if  $b_{ii} = 1$ , and  $b_i = 1$  if  $b_{ii} = 0$ .

We claim that  $R$  is different from each set in the list.

Each bit string is unique, and  $R$  and  $S_i$  differ in the  $i$ -th bit for all  $i$ .

# Schröder-Bernstein Theorem

## ■ Theorem

If  $A$  and  $B$  are sets with  $|A| \leq |B|$  and  $|B| \leq |A|$ , then  $|A| = |B|$ . In other words, if there are one-to-one functions  $f$  from  $A$  to  $B$  and  $g$  from  $B$  to  $A$ , then there is a one-to-one correspondence between  $A$  and  $B$ .



# Schröder-Bernstein Theorem

## ■ Theorem

If  $A$  and  $B$  are sets with  $|A| \leq |B|$  and  $|B| \leq |A|$ , then  $|A| = |B|$ . In other words, if there are one-to-one functions  $f$  from  $A$  to  $B$  and  $g$  from  $B$  to  $A$ , then there is a one-to-one correspondence between  $A$  and  $B$ .

## Example

Show that  $|(0, 1)| = |(0, 1]|$ .

# Schröder-Bernstein Theorem

## ■ Theorem

If  $A$  and  $B$  are sets with  $|A| \leq |B|$  and  $|B| \leq |A|$ , then  $|A| = |B|$ . In other words, if there are one-to-one functions  $f$  from  $A$  to  $B$  and  $g$  from  $B$  to  $A$ , then there is a one-to-one correspondence between  $A$  and  $B$ .

## Example

Show that  $|(0, 1)| = |(0, 1]|$ .

$$f(x) = x; \quad g(x) = x/2$$

# Computable vs Uncomputable

## ■ Definition

We say that a function is *computable* if there is a computer program in some programming language that finds the values of this function. If a function is **not** computable, we say it is *uncomputable*.

# Computable vs Uncomputable

## ■ Definition

We say that a function is *computable* if there is a computer program in some programming language that finds the values of this function. If a function is **not** computable, we say it is *uncomputable*.

## Theorem

There are functions that are **not** computable.

# Computable vs Uncomputable

## ■ Definition

We say that a function is *computable* if there is a computer program in some programming language that finds the values of this function. If a function is **not** computable, we say it is *uncomputable*.

## Theorem

There are functions that are **not** computable.

## Cantor's theorem

If  $S$  is a set, then  $|S| < |\mathcal{P}(S)|$ .

# Next Lecture

- complexity ...

