

# Cardinality of Sets

Section 2.5

## Section Summary

- Cardinality
- Countable Sets
- Computability

## Cardinality

**Definition:** The *cardinality* of a set  $A$  is equal to the cardinality of a set  $B$ , denoted

$$|A| = |B|,$$

if and only if there is a one-to-one correspondence (*i.e.*, a bijection) from  $A$  to  $B$ .

- If there is a one-to-one function (*i.e.*, an injection) from  $A$  to  $B$ , the cardinality of  $A$  is less than or the same as the cardinality of  $B$  and we write  $|A| \leq |B|$ .
- When  $|A| \leq |B|$  and  $A$  and  $B$  have different cardinality, we say that the cardinality of  $A$  is less than the cardinality of  $B$  and write  $|A| < |B|$ .

## Cardinality

- **Definition:** 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 *uncountable*.
- The set of real numbers  $\mathbf{R}$  is an uncountable set.
- When an infinite set is countable (*countably infinite*) its cardinality is  $\aleph_0$  (where  $\aleph$  is aleph, the 1<sup>st</sup> letter of the Hebrew alphabet). We write  $|S| = \aleph_0$  and say that  $S$  has cardinality “aleph null.”

## Showing that a Set is Countable

- An infinite set is countable if and only if it is possible to list the elements of the set in a sequence (indexed by the positive integers).
- The reason for this is that a one-to-one correspondence  $f$  from the set of positive integers to a set  $S$  can be expressed in terms of a sequence  $a_1, a_2, \dots, a_n, \dots$  where  $a_1 = f(1)$ ,  $a_2 = f(2)$ ,  $\dots$ ,  $a_n = f(n)$ ,  $\dots$

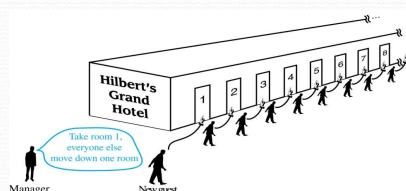
## Hilbert's Grand Hotel



David Hilbert

The Grand Hotel (example due to David Hilbert) 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?

**Explanation:** Because the rooms of Grand Hotel are countable, we can list them as Room 1, Room 2, Room 3, and so on. When a new guest arrives, we move the guest in Room 1 to Room 2, the guest in Room 2 to Room 3, and in general the guest in Room  $n$  to Room  $n + 1$ , for all positive integers  $n$ . This frees up Room 1, which we assign to the new guest, and all the current guests still have rooms.

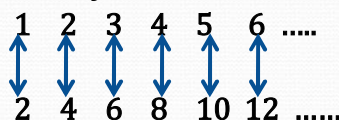


The hotel can also accommodate a countable number of new guests, all the guests on a countable number of buses where each bus contains a countable number of guests (see exercises).

## Showing that a Set is Countable

**Example 1:** Show that the set of positive even integers  $E$  is countable set.

**Solution:** Let  $f(x) = 2x$ .



Then  $f$  is a bijection from  $\mathbf{N}$  to  $E$  since  $f$  is both one-to-one and onto. To show that it is one-to-one, suppose that  $f(n) = f(m)$ . Then  $2n = 2m$ , and so  $n = m$ . To see that it is onto, suppose that  $t$  is an even positive integer. Then  $t = 2k$  for some positive integer  $k$  and  $f(k) = t$ . ◀

## Showing that a Set is Countable

**Example 2:** Show that the set of integers  $\mathbf{Z}$  is countable.

**Solution:** Can list in a sequence:

0, 1, -1, 2, -2, 3, -3, .....

Or can define a bijection from  $\mathbf{N}$  to  $\mathbf{Z}$ :

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

## The properties of Cardinality of infinite set

For every sets A and B, the following equivalence  
Are held:

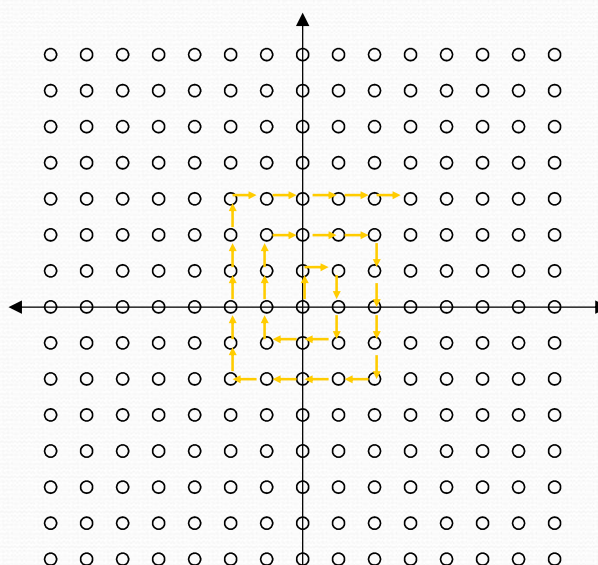
- (a)  $|A| = |B|$ ;  $|A| < |B|$ ;  $|A| > |B|$
- (b) If  $|A| \leq |B|$  and  $|B| \leq |A|$ , then  $|A| = |B|$   
(Benstien theorem)

If we want to prove  $|A| = |B|$ , we usually first prove  
 $|A| \leq |B|$  and then prove  $|B| \leq |A|$

The following example is interesting.

## ordered pairs of integers are countably infinite

A one-to-one  
correspondence





## The Positive Rational Numbers are Countable

- **Definition:** A rational number can be expressed as the ratio of two integers  $p$  and  $q$  such that  $q \neq 0$ .

- $\frac{3}{4}$  is a rational number
- $\sqrt{2}$  is not a rational number.

**Example 3:** Show that the positive rational numbers are countable.

**Solution:** The positive rational numbers are countable since they can be arranged in a sequence:

$$r_1, r_2, r_3, \dots$$

The next slide shows how this is done.  $\rightarrow$

## The Positive Rational Numbers are Countable

First row  $q = 1$ .  
Second row  $q = 2$ .  
etc.

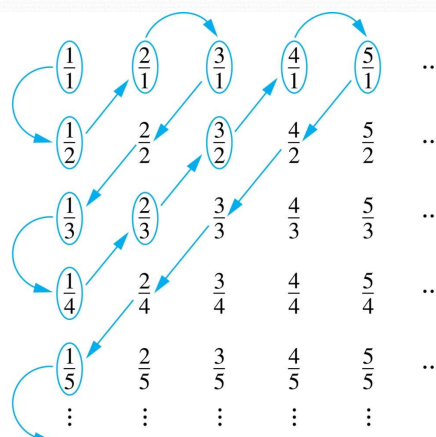
### Constructing the List

First list  $p/q$  with  $p + q = 2$ .  
Next list  $p/q$  with  $p + q = 3$

And so on.

$1, \frac{1}{2}, 2, 3, \frac{1}{3}, \frac{1}{4}, \frac{2}{3}, \dots$

Terms not circled are not listed because they repeat previously listed terms



## 2.5 Cardinality of Sets

The set of positive rational numbers  $Q^+$  (another solution)

- $\forall x \in Q^+, x = p/q, p, q \in Z^+$
- Let  $S = \{ (p, q) \mid p, q \in Z^+ \} = Z^+ \times Z^+$ .

■

$$\left. \begin{array}{l} |Q^+| \leq |S| \\ |S| = |Z^+| \\ |Z^+| \leq |Q^+| \end{array} \right\} \Rightarrow |Q^+| = |Z^+|$$

13

## 2.5 Cardinality of Sets

$$(1) |Q^+| \leq |S|$$

Suppose that  $r = \frac{p}{q} \in Q^+$

$\frac{p}{q} \rightarrow (p, q)$  is injective

$$\therefore |Q^+| \leq |S|$$

14

## 2.5 Cardinality of Sets

(2)  $|S| = |Z^+|$  **An infinite set is countable iff it is possible to list all the elements of the set in a sequence**

	1	2	3	...	p	...
1	(1,1)	(2,1)	(3,1)	...	(p,1)	...
2	(1,2)	(2,2)	(3,2)	...	(p,2)	...
3	(1,3)	(2,3)	(3,3)	...	(p,3)	...
...	...	...	...	...	...	...
q	(1,q)	(2,q)	(3,q)	...	(p,q)	...
...	...	...	...	...	...	...

$$1 + 2 + \dots + (p+q-2) = \frac{(p+q-2)(p+q-1)}{2}$$

$$n = \frac{1}{2}(p+q-2)(p+q-1) + q$$

15

## 2.5 Cardinality of Sets

(3)  $|Z^+| \leq |Q^+|$

$$\because Z^+ \subseteq Q^+$$

$$\therefore |Z^+| \leq |Q^+|$$

**Note :**

- (1) There are the same number of positive rational numbers and positive integers.
- (2) The set of all rational numbers Q, positive and negative, is countable infinite.

16



## Strings

**Example 4:** Show that the set of finite strings  $S$  over a finite alphabet  $A$  is countably infinite.

Assume an alphabetical ordering of symbols in  $A$

**Solution:** Show that the strings can be listed in a sequence. First list

1. All the strings of length 0 in alphabetical order.
2. Then all the strings of length 1 in lexicographic (as in a dictionary) order.
3. Then all the strings of length 2 in lexicographic order.
4. And so on.

This implies a bijection from  $\mathbb{N}$  to  $S$  and hence it is a countably infinite set. ◀

## The set of all Java programs is countable.

**Example 5:** Show that the set of all Java programs is countable.

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

- Feed the string into a Java compiler. (A Java compiler will determine if the input program is a syntactically correct Java program.)
- If the compiler says YES, this is a syntactically correct Java program, we add the program to the list.
- We move on to the next string.

In this way we construct an implied bijection from  $\mathbb{N}$  to the set of Java programs. Hence, the set of Java programs is countable. ◀

### The properties of the countable sets:

- 1) No infinite set has a smaller cardinality than a countable set.
- 2) The union of two countable sets is countable.
- 3) The union of finite number of countable sets is countable.
- 4) The union of a countable number of countable sets is countable.

19

### 3. Cantor Diagonalization Argument

---- An important technique used to construct an object which is not a member of a countable set of objects

**【Theorem】** The set of real numbers between 0 and 1 is uncountable.

*Proof:*

$$A = \{x \mid x \in (0,1) \wedge x \in R\}$$

$$\left. \begin{array}{l} (1) |Z^+| \leq |A| \\ (2) |Z^+| \neq |A| \end{array} \right\} \longrightarrow |Z^+| < |A|$$

20

## 2.5 Cardinality of Sets

$$(1) |Z^+| \leq |A|$$

$$A = \{x \mid x \in (0,1) \wedge x \in R\}$$

$$B = \left\{ \frac{1}{n+1} \mid n \in Z^+ \right\}$$

$$\therefore |B| = |Z^+| \quad B \subseteq A$$

$$\therefore |Z^+| \leq |A|$$

21

## 2.5 Cardinality of Sets

$$(2) |Z^+| \neq |A|$$

Assume A is countable, then let  $A = \{r_1, r_2, r_3, \dots, r_n, \dots\}$

Represent each real number in the list using *its decimal expansion*.

e.g.,  $1/3 = .3333333\dots$ ,  $1/2 = .5000000\dots = .4999999\dots$

THE LIST....

$$r_1 = 0.\mathbf{d_{11}}d_{12}d_{13}d_{14}d_{15}d_{16}\dots$$

$$r_2 = 0.d_{21}\mathbf{d_{22}}d_{23}d_{24}d_{25}d_{26}\dots$$

$$r_3 = 0.d_{31}d_{32}\mathbf{d_{33}}d_{34}d_{35}d_{36}\dots$$

...

Now construct the number  $x = 0.x_1x_2x_3x_4x_5x_6x_7\dots$

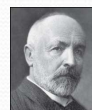
$$x_i = 3 \text{ if } d_{ii} \neq 3$$

$$x_i = 4 \text{ if } d_{ii} = 3$$

Then x is not equal to any number in the list.

Hence, no such list can exist and hence the interval (0,1) is uncountable .

Georg Cantor  
(1845-1918)



22

## 2.5 Cardinality of Sets

**【Theorem】** The set of real numbers  $R = (-\infty, +\infty)$  has the same cardinality as the set  $(0,1)$ .

*Proof:*

Let  $f(x) = \tan(x)$ .

$f(x)$  is a bijection from  $(-\frac{\pi}{2}, \frac{\pi}{2})$  to  $R = (-\infty, +\infty)$ .

$$\because \left| \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \right| = |(0,1)| \quad \therefore |R| = |(0,1)|$$

$$|R| = \aleph_1$$

23

## 2.5 Cardinality of Sets

【Example】 Suppose that  $[0,1] = \{x \mid x \in R, 0 \leq x \leq 1\}$ . Show that the cardinality of this set is  $\aleph_1$ .

*Proof:*

$$A = [0,1] = \{x \mid x \in R, 0 \leq x \leq 1\}$$

$$B = (0,1) = \{x \mid x \in R, 0 < x < 1\}$$

$$(1) B \subseteq A \Rightarrow |B| \leq |A|$$

$$(2) \text{ Let } g(x) = \frac{1}{2}x + \frac{1}{4}, x \in [0,1]$$

Hence,  $g(x)$  is a bijection from  $[0,1]$  to  $[1/4, 3/4]$ .

$$\text{Thus } |A| \leq |B|$$

24

## 2.5 Cardinality of Sets

**【Schröder-Bernstein 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  $B$ .

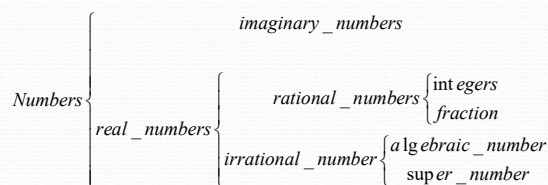
**【Theorem】** The cardinality of the power set of an arbitrary set has a greater cardinality than the original arbitrary set.

#### The Continuum Hypothesis

The continuum hypothesis (CH) asserts that there is no cardinal number  $a$  such that  $\aleph_0 < a < \aleph_1$ .

25

## Classification of numbers





## Computability (Optional)

- **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**.
- There are uncomputable functions. We have shown that the set of Java programs is countable. Exercise 38 in the text shows that there are uncountably many different functions from a particular countably infinite set (i.e., the positive integers) to itself. Therefore (Exercise 39) there must be uncomputable functions.

## Homework

Sec. 2.5 4(c,d), 28 , 36, 38

# Matrices

(此节自学，作业要做)

Section 2.6

## Section Summary

- Definition of a Matrix
- Matrix Arithmetic
- Transposes and Powers of Arithmetic
- Zero-One matrices

## Matrices

- Matrices are useful discrete structures that can be used in many ways. For example, they are used to:
  - describe certain types of functions known as linear transformations.
  - Express which vertices of a graph are connected by edges (see Chapter 10).
- In later chapters, we will see matrices used to build models of:
  - Transportation systems.
  - Communication networks.
- Algorithms based on matrix models will be presented in later chapters.
- Here we cover the aspect of matrix arithmetic that will be needed later.

## Matrix

**Definition:** A *matrix* is a rectangular array of numbers. A matrix with  $m$  rows and  $n$  columns is called an  $m \times n$  matrix.

- The plural of matrix is *matrices*.
- A matrix with the same number of rows as columns is called *square*.
- Two matrices are *equal* if they have the same number of rows and the same number of columns and the corresponding entries in every position are equal.

$3 \times 2$  matrix

$$\begin{bmatrix} 1 & 1 \\ 0 & 2 \\ 1 & 3 \end{bmatrix}$$

## Notation

- Let  $m$  and  $n$  be positive integers and let

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

- The  $i$ th row of  $\mathbf{A}$  is the  $1 \times n$  matrix  $[a_{i1}, a_{i2}, \dots, a_{in}]$ . The  $j$ th column of  $\mathbf{A}$  is the  $m \times 1$  matrix:

$$\begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}$$

- The  $(i,j)$ th element or entry of  $\mathbf{A}$  is the element  $a_{ij}$ . We can use  $\mathbf{A} = [a_{ij}]$  to denote the matrix with its  $(i,j)$ th element equal to  $a_{ij}$ .

## Matrix Arithmetic: Addition

**Definition:** Let  $\mathbf{A} = [a_{ij}]$  and  $\mathbf{B} = [b_{ij}]$  be  $m \times n$  matrices. The sum of  $\mathbf{A}$  and  $\mathbf{B}$ , denoted by  $\mathbf{A} + \mathbf{B}$ , is the  $m \times n$  matrix that has  $a_{ij} + b_{ij}$  as its  $(i,j)$ th element. In other words,  $\mathbf{A} + \mathbf{B} = [a_{ij} + b_{ij}]$ .

**Example:**

$$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 2 & -3 \\ 3 & 4 & 0 \end{bmatrix} + \begin{bmatrix} 3 & 4 & -1 \\ 1 & -3 & 0 \\ -1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 4 & -2 \\ 3 & -1 & -3 \\ 2 & 5 & 2 \end{bmatrix}$$

Note that matrices of different sizes can not be added.

## Matrix Multiplication

**Definition:** Let  $\mathbf{A}$  be an  $n \times k$  matrix and  $\mathbf{B}$  be a  $k \times n$  matrix. The *product* of  $\mathbf{A}$  and  $\mathbf{B}$ , denoted by  $\mathbf{AB}$ , is the  $n \times n$  matrix that has its  $(i,j)$ th element equal to the sum of the products of the corresponding elements from the  $i$ th row of  $\mathbf{A}$  and the  $j$ th column of  $\mathbf{B}$ . In other words, if  $\mathbf{AB} = [c_{ij}]$  then  $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{ik}b_{kj}$ .

**Example:**

$$\begin{bmatrix} 1 & 0 & 4 \\ 2 & 1 & 1 \\ 3 & 1 & 0 \\ 0 & 2 & 2 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 1 & 1 \\ 3 & 0 \end{bmatrix} = \begin{bmatrix} 14 & 4 \\ 8 & 9 \\ 7 & 13 \\ 8 & 2 \end{bmatrix}$$

The product of two matrices is undefined when the number of columns in the first matrix is not the same as the number of rows in the second.

## Illustration of Matrix Multiplication

- The Product of  $\mathbf{A} = [a_{ij}]$  and  $\mathbf{B} = [b_{ij}]$

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{ik} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mk} \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1j} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2j} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ b_{k1} & b_{k2} & \dots & b_{kj} & \dots & b_{kn} \end{bmatrix}$$

$$\mathbf{AB} = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{ij} & & & \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \dots & c_{mn} \end{bmatrix}$$

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{ik}b_{kj}$$



## Matrix Multiplication is not Commutative

**Example:** Let

$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

Does  $\mathbf{AB} = \mathbf{BA}$ ?

**Solution:**

$$\mathbf{AB} = \begin{bmatrix} 2 & 2 \\ 5 & 3 \end{bmatrix} \quad \mathbf{BA} = \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix}$$

$$\mathbf{AB} \neq \mathbf{BA}$$

## Identity Matrix and Powers of Matrices

**Definition:** The *identity matrix of order  $n$*  is the  $m \times n$  matrix  $\mathbf{I}_n = [\delta_{ij}]$ , where  $\delta_{ij} = 1$  if  $i = j$  and  $\delta_{ij} = 0$  if  $i \neq j$ .

$$\mathbf{I}_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

$$\mathbf{AI}_n = \mathbf{I}_m \mathbf{A} = \mathbf{A}$$

when  $\mathbf{A}$  is an  $m \times n$  matrix

Powers of square matrices can be defined. When  $\mathbf{A}$  is an  $n \times n$  matrix, we have:

$$\mathbf{A}^0 = \mathbf{I}_n \quad \mathbf{A}^r = \underbrace{\mathbf{A} \mathbf{A} \mathbf{A} \dots \mathbf{A}}_{r \text{ times}}$$

## Transposes of Matrices

**Definition:** Let  $\mathbf{A} = [a_{ij}]$  be an  $m \times n$  matrix. The *transpose* of  $\mathbf{A}$ , denoted by  $\mathbf{A}^t$ , is the  $n \times m$  matrix obtained by interchanging the rows and columns of  $\mathbf{A}$ .

If  $\mathbf{A}^t = [b_{ij}]$ , then  $b_{ij} = a_{ji}$  for  $i = 1, 2, \dots, n$   
and  $j = 1, 2, \dots, m$ .

The transpose of the matrix  $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$  is the matrix  $\begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$ .

## Transposes of Matrices

**Definition:** A square matrix  $\mathbf{A}$  is called symmetric if  $\mathbf{A} = \mathbf{A}^t$ . Thus  $\mathbf{A} = [a_{ij}]$  is symmetric if  $a_{ij} = a_{ji}$  for  $i$  and  $j$  with  $1 \leq i \leq n$  and  $1 \leq j \leq n$ .

The matrix  $\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$  is square.

Square matrices do not change when their rows and columns are interchanged.

## Zero-One Matrices

**Definition:** A matrix all of whose entries are either 0 or 1 is called a *zero-one matrix*. (These will be used in Chapters 9 and 10.)

Algorithms operating on discrete structures represented by zero-one matrices are based on Boolean arithmetic defined by the following Boolean operations:

$$b_1 \wedge b_2 = \begin{cases} 1 & \text{if } b_1 = b_2 = 1 \\ 0 & \text{otherwise} \end{cases} \quad b_1 \vee b_2 = \begin{cases} 1 & \text{if } b_1 = 1 \text{ or } b_2 = 1 \\ 0 & \text{otherwise} \end{cases}$$

## Zero-One Matrices

**Definition:** Let  $\mathbf{A} = [a_{ij}]$  and  $\mathbf{B} = [b_{ij}]$  be an  $m \times n$  zero-one matrices.

- The *join* of  $\mathbf{A}$  and  $\mathbf{B}$  is the zero-one matrix with  $(i,j)$ th entry  $a_{ij} \vee b_{ij}$ . The *join* of  $\mathbf{A}$  and  $\mathbf{B}$  is denoted by  $\mathbf{A} \vee \mathbf{B}$ .
- The *meet* of  $\mathbf{A}$  and  $\mathbf{B}$  is the zero-one matrix with  $(i,j)$ th entry  $a_{ij} \wedge b_{ij}$ . The *meet* of  $\mathbf{A}$  and  $\mathbf{B}$  is denoted by  $\mathbf{A} \wedge \mathbf{B}$ .

## Joins and Meets of Zero-One Matrices

**Example:** Find the join and meet of the zero-one matrices

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

**Solution:** The join of  $\mathbf{A}$  and  $\mathbf{B}$  is

$$\mathbf{A} \vee \mathbf{B} = \begin{bmatrix} 1 \vee 0 & 0 \vee 1 & 1 \vee 0 \\ 0 \vee 1 & 1 \vee 1 & 0 \vee 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

The meet of  $\mathbf{A}$  and  $\mathbf{B}$  is

$$\mathbf{A} \wedge \mathbf{B} = \begin{bmatrix} 1 \wedge 0 & 0 \wedge 1 & 1 \wedge 0 \\ 0 \wedge 1 & 1 \wedge 1 & 0 \wedge 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

## Boolean Product of Zero-One Matrices

**Definition:** Let  $\mathbf{A} = [a_{ij}]$  be an  $m \times k$  zero-one matrix and  $\mathbf{B} = [b_{ij}]$  be a  $k \times n$  zero-one matrix. The *Boolean product* of  $\mathbf{A}$  and  $\mathbf{B}$ , denoted by  $\mathbf{A} \odot \mathbf{B}$ , is the  $m \times n$  zero-one matrix with  $(i,j)$ th entry

$$c_{ij} = (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \dots \vee (a_{ik} \wedge b_{kj}).$$

**Example:** Find the Boolean product of  $\mathbf{A}$  and  $\mathbf{B}$ , where

$$\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Continued on next slide  $\rightarrow$



## Boolean Product of Zero-One Matrices

**Solution:** The Boolean product  $\mathbf{A} \odot \mathbf{B}$  is given by

$$\begin{aligned}\mathbf{A} \odot \mathbf{B} &= \begin{bmatrix} (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \\ (0 \wedge 1) \vee (1 \wedge 0) & (0 \wedge 1) \vee (1 \wedge 1) & (0 \wedge 0) \vee (1 \wedge 1) \\ (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \end{bmatrix} \\ &= \begin{bmatrix} 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \\ 0 \vee 0 & 0 \vee 1 & 0 \vee 1 \\ 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.\end{aligned}$$

## Boolean Powers of Zero-One Matrices

**Definition:** Let  $\mathbf{A}$  be a square zero-one matrix and let  $r$  be a positive integer. The  $r$ th Boolean power of  $\mathbf{A}$  is the Boolean product of  $r$  factors of  $\mathbf{A}$ , denoted by  $\mathbf{A}^{[r]}$ . Hence,

$$\mathbf{A}^{[r]} = \underbrace{\mathbf{A} \odot \mathbf{A} \odot \dots \odot \mathbf{A}}_{r \text{ times}}.$$

We define  $\mathbf{A}^{[0]}$  to be  $\mathbf{I}_n$ .

(The Boolean product is well defined because the Boolean product of matrices is associative.)



## Boolean Powers of Zero-One Matrices

**Example:** Let  $A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$ .

Find  $A^n$  for all positive integers  $n$ .

**Solution:**

$$A^{[2]} = A \odot A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad A^{[3]} = A^{[2]} \odot A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

$$A^{[4]} = A^{[3]} \odot A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$$A^{[5]} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad A^{[n]} = A^5 \quad \text{for all positive integers } n \text{ with } n \geq 5.$$

## Homework

Sec. 2.6 27