

**4190.101**

# **Discrete Mathematics**

Chapter 2 Basic Structures: Sets, Functions,  
Sequences, Sums, and Matrices

Gunhee Kim

# 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 some subset of natural numbers ( $\mathbf{N}$ ) 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  $a_1 = f(1)$ ,  $a_2 = f(2)$ , ...,  $a_n = f(n)$ , ...

# Hilbert's Grand Hotel

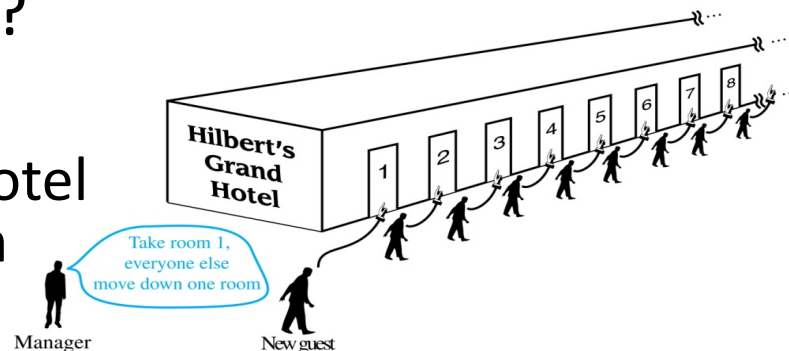


David Hilbert

- 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?

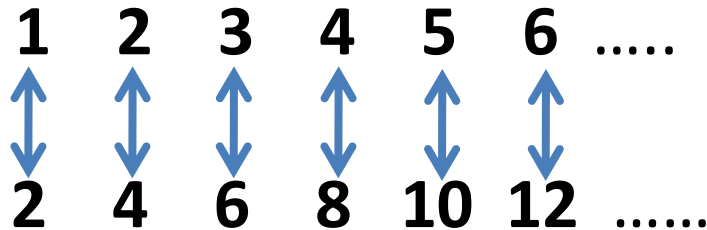
- **Explanation**

- 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 R2 to R3, 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.



# 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 **Z** is countable.
- **Solution:** can list in a sequence:  
0, 1, - 1, 2, - 2, 3, - 3 ,.....
- Or can define a bijection from **N** to **Z**:
  - When  $n$  is even:  $f(n) = n/2$
  - When  $n$  is odd:  $f(n) = -(n-1)/2$



# 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.



# The Positive Rational Numbers are Countable

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

## Constructing the List

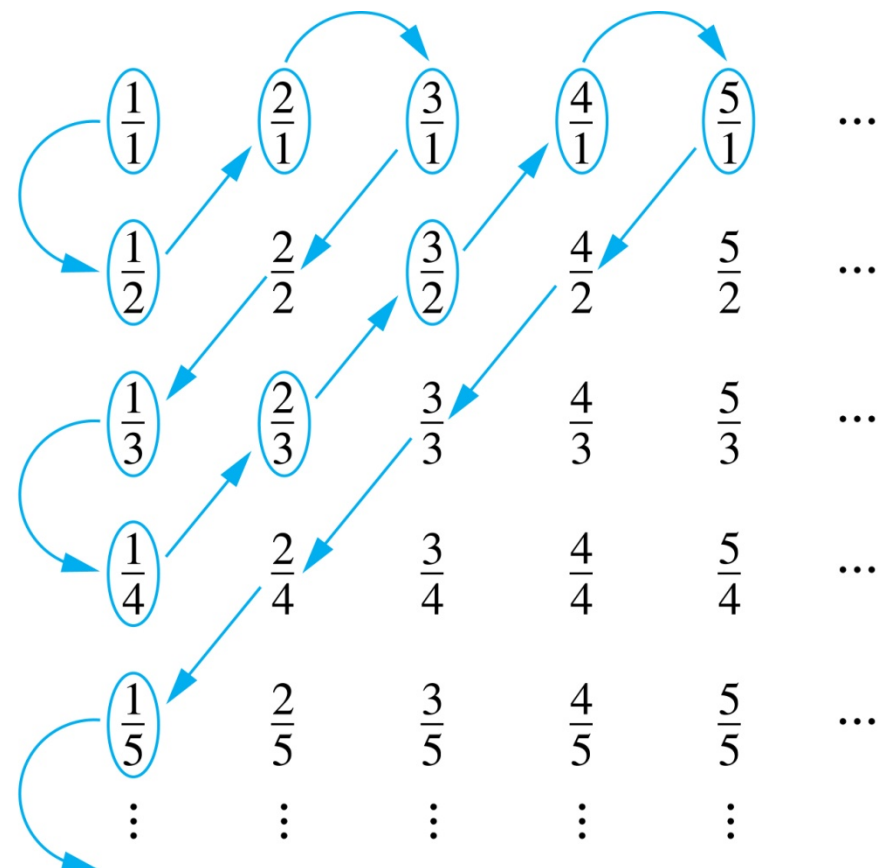
First list  $p/q$  with  $p + q = 2$ .

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



# Strings

- **Example 4:** Show that the set of finite strings  $S$  over the lowercase letters is countably infinite.
- **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  $\mathbf{N}$  to  $S$  and hence it is a countably infinite set.

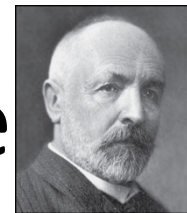


# The set of all Java programs is countable

- **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  $\mathbf{N}$  to the set of Java programs. Hence, the set of Java programs is countable.



# The Real Numbers are Uncountable



Georg Cantor  
(1845-1918)

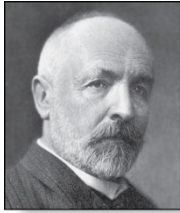
- Show that the set of real numbers is uncountable.
- **Solution:** The method is called the Cantor diagonalization argument, and is a proof by contradiction.
  1. Suppose  $\mathbf{R}$  is countable. Then the real numbers between 0 and 1 are also countable (any subset of a countable set is countable - an exercise in the textbook).
  2. The real numbers btw 0 and 1 can be listed in order  $r_1, r_2, r_3, \dots, r_n, \dots$ .
  3. Let the decimal representation of this listing be

$$\begin{aligned}
 r_1 &= 0.d_{11}d_{12}d_{13}d_{14}\dots \\
 r_2 &= 0.d_{21}d_{22}d_{23}d_{24}\dots \\
 r_3 &= 0.d_{31}d_{32}d_{33}d_{34}\dots \\
 r_4 &= 0.d_{41}d_{42}d_{43}d_{44}\dots \\
 &\dots
 \end{aligned}$$

4. However, given this list we can now construct a new real number  $r_q$  between 0 and 1 that does not appear on this list,

$$\begin{aligned}
 r_q &= 0.d_{q1}d_{q2}d_{q3}\dots d_{qn}\dots \\
 &\text{with } d_{q1} \neq d_{11}, d_{q2} \neq d_{22}, d_{q3} \neq d_{33}, \dots
 \end{aligned}$$

# The Real Numbers are Uncountable



Georg Cantor  
(1845-1918)

- Show that the set of real numbers is uncountable.
- **Solution:** The method is called the Cantor diagonalization argument, and is a proof by contradiction.
  5. With this construction  $r_q$  differs from any real number on the list in at least one position.
  6. Since a set with an uncountable subset is uncountable (an exercise), the set of real numbers is uncountable. ◀

# Matrices

## 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.

# Matrices

- **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.

$$3 \times 2 \text{ matrix} \quad \begin{bmatrix} 1 & 1 \\ 0 & 2 \\ 1 & 3 \end{bmatrix}$$

# Notation

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

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

- 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:

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

- 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  $\mathbf{B} = [b_{ij}]$

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

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

# 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  $\mathbf{I}_n = [I_{ij}]$ , where  $I_{ij} = 1$  if  $i = j$  and  $I_{ij} = 0$  if  $i \neq j$ .

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

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

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:

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

# Transpose 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.

- Symmetric 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:

# 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  $\mathbf{A} \wedge \mathbf{B}$ .

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

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

# 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

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

$$= \begin{bmatrix} 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \\ 0 \vee 0 & 0 \vee 1 & 0 \vee 1 \\ 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$



# Boolean Product 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 Product of Zero-One Matrices

- **Example:** Let

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

Find  $\mathbf{A}^{[n]}$  for all positive integers  $n$ .

- **Solution:**

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

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

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