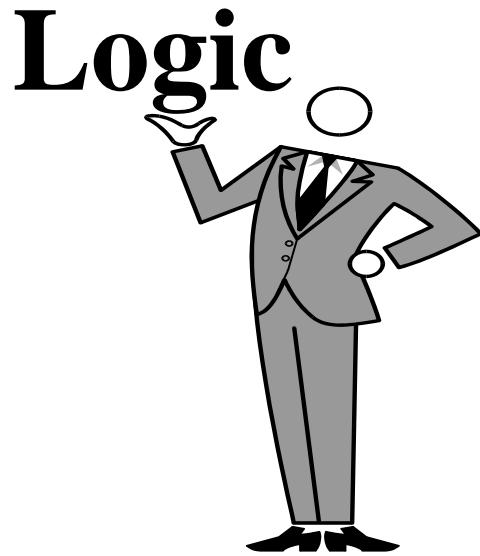


Mat2033 - Discrete Mathematics

The Foundations: Logic and Proof, Sets and Functions

Sections 1.1, 1.2



Propositional Equivalences

Propositions

A **proposition** is a statement that is either true or false, but not both.

Today is Tuesday.

Six is a prime number.

Are you Bob?

7<5

Consider this statement.

Example: All the following statements are propositions

1. Washington D.C., is the capital of the United States of America. (True).
2. Toronto is the capital of Canada. (False)
3. $1+1=2$ (True)
4. $2+2=3$ (False)

2

Example: Consider the following sentences.

1. What time is it? (Not Proposition)
2. Read this carefully. (Not Proposition)
3. $x+1=2$ (Not Proposition)
4. $x+y=z$ (Not Proposition)

Compound Propositions

Compound propositions are formed from existing propositions using logical operators

Today is Wednesday and it is snowing outside.

12 is not a prime number.

Negation of a Proposition

P	$\neg P$	NOT
T	F	
F	T	

3

Example: Find the negation of the proposition
"Today is Friday"

and express this in simple English.

Solution: The negation is

"It is not the case that today is Friday."

This negation can be more simply expressed by

"Today is not Friday" or "It is not Friday Today".

introduce the logical operators that are used to form new propositions from two or more existing propositions. These logical operators are also called connectives.

Definition 3: Let p and q be propositions. The proposition " p or q ," denoted by $p \vee q$, is the proposition that is false when p and q are both false and true otherwise. The proposition $p \vee q$ is called the disjunction of p and q .

Disjunction of Two Propositions

p	q	$p \vee q$	OR
T	T	T	
T	F	T	
F	T	T	
F	F	F	

- The binary *disjunction operator* “ \vee ” (*OR*) combines two propositions to form their logical *disjunction*.
- $p =$ “My car has a bad engine.”
- $q =$ “My car has a bad carburetor.”
- $p \vee q =$ “Either my car has a bad engine, or my car has a bad carburetor.”

Definition 2: Let p and q be propositions. The proposition " p and q " , denoted by $p \wedge q$, is the proposition that is true when both p and q are true and is false otherwise. The proposition $p \wedge q$ is called the conjunction of p and q .

Conjunction of Two Propositions

p	q	$p \wedge q$	AND
T	T	T	
T	F	F	
F	T	F	
F	F	F	

Example: Find the conjunction of the propositions p and q where p is the proposition "Today is Friday" and q is the proposition "It is raining today".

Solution: The conjunction of these propositions, $p \wedge q$, is the proposition "Today is Friday and it is raining today".

This proposition is true on rainy Fridays and is false on any day that is not a Friday and on Fridays when it does not rain.

Definition 4: Let p and q be propositions. The exclusive OR of p and q , denoted by $P \oplus q$, is the proposition that is true when exactly one of p and q is true and is false otherwise.

Exclusive OR of Two Propositions

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Exactly
one of
them is
true.

For example, the inclusive or is being used in the statement

"Students who have taken calculus or computer science can take this class."

Here we mean that students who have taken both calculus and computer science can take the class, as well as the students who have taken only one of the two subjects. On the other hand, we are using the exclusive or when we say

"Students who have taken calculus or computer science, but not both, can enroll in this class."

Here we mean that the students who have taken both calculus and a computer science course cannot take the class. Only those who have taken exactly one of the two courses can take the class.

Similarly, when a menu at a restaurant states, "Soup or salad comes with an entrée," the restaurant almost always means that customers can have either soup or salad, but not both. Hence, it is an exclusive, rather than an inclusive or.

Definition 5: Let p and q be propositions. The implication $p \rightarrow q$ is the proposition that is false when p is true and q is false and true otherwise. In this implication p is called the hypothesis (or antecedent or premise) and q is called the conclusion (or consequence).

Implication

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

p is called the *hypothesis* and q is the *conclusion*

Implication

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

- “if p , then q ”
- “ p implies q ”
- “if p,q ”
- “ p only if q ”
- “ p is sufficient for q ”
- “ q if p ”
- “ q whenever p ”
- “ q is necessary for p ”

q whenever p

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Suppose that the proposition is true.
Then, q is true whenever p is true.

p is sufficient for q

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Suppose that the proposition is true. Then, to guarantee that q is true it is sufficient to say that p is true.

Note that $p \rightarrow q$ is false only in the case that p is true but q is false, so that it is true when both p and q are true, and when p is false (no matter what truth value q has).

For instance, the implication

"If it is sunny today, then we will go to beach."

is an implication used in normal language, since there is a relationship between the hypothesis and the conclusion. Further, this implication is considered valid unless it is indeed sunny today, but we do not go to beach. On the other hand, the implication

"If today is Friday, then $2+3=5$."

is true from the definition of implication, since its conclusion is true. (The truth value of the hypothesis does not matter then.) The implication

"If today is Friday, then $2+3=6$ "

is true everyday except Friday, even though $2+3=6$ is false.

Examples of Implications

- “If this lecture ends, then the sun will rise tomorrow.” *True or False?*
- “If Tuesday is a day of the week, then I am a penguin.” *True or False?*
- “If $1+1=6$, then Bush is president.”
True or False?
- “If the moon is made of green cheese, then I am richer than Bill Gates.” *True or False?*

We can build up compound propositions using the negation operator and different connectives defined so far.
For instance

(*) $(p \vee q) \wedge (\neg r)$ is the conjunction of $p \vee q$ and $\neg r$

(**) $\neg p \wedge q$ is the conjunction of $\neg p$ and q . (Not the negation of the conjunction of p and q , namely $\neg(p \wedge q)$.)

There are some related implications that can be formed from $p \rightarrow q$. The proposition $q \rightarrow p$ is called the converse of $p \rightarrow q$. The contrapositive of $p \rightarrow q$ is the proposition $\neg q \rightarrow \neg p$.

Example: Find the converse and the contrapositive of the implication

"If today is Thursday, then I have a test today."

Solution: The converse is

"If I have a test today, then today is Thursday."

And the contrapositive of this implication is

"If I have not a test today, then today is not Thursday"

Converse of an Implication

p	q	$p \rightarrow q$	$p \leftarrow q$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

And
Conversely



Example of Converse

If it stays warm for a week, the apple trees will bloom.

If the apple trees bloom, it will be warm for a week.

If x is even then x^2 is even.

If x^2 is even then x is even.

Contrapositive of an Implication

p	q	$p \rightarrow q$	$\neg p$	$\neg q$	$\neg q \rightarrow \neg p$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	F	T
F	F	T	T	T	T

Examples of Contrapositive

If it snows tonight, then I will stay at home.

If I do not stay at home, then it will not snow tonight.

If x is odd then x^2 is odd.

If x^2 is not odd then x is not odd.

If x^2 is even then x is even.

Definition 6: Let p and q be propositions. The biconditional $p \leftrightarrow q$ is the proposition that is true when p and q have the same truth values and is false otherwise.

TABLE 6 : The truth table for the biconditional $p \leftrightarrow q$		
p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Note that the biconditional $p \leftrightarrow q$ is true precisely when both the implications $p \rightarrow q$ and $q \rightarrow p$ are true. Because of this, the terminology

" p if and only if q "

is used for this biconditional. Other common ways of expressing the proposition $p \leftrightarrow q$ are:

" p is necessary and sufficient for q " and

"If P then q , and conversely."

Biconditional

$$p \leftrightarrow q$$

p	q	$p \rightarrow q$	$p \leftarrow q$	$(p \rightarrow q) \wedge (p \leftarrow q)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Biconditional

$$p \leftrightarrow q \quad (p \rightarrow q) \wedge (p \leftarrow q)$$

p if and only if **q**

p iff **q**

Translating English Sentences:

English is often ambiguous. Translating sentences into logical expressions removes the ambiguity.

Example: "You can access the Internet from Campus only if you are a computer science major or you are not a freshman."

Translate this sentence into a logical expression.

Example: "You can access the Internet from Campus only if you are a computer science major or you are not a freshman."

Translate this sentence into a logical expression.

Solution:

a = You can access the Internet from Campus

c = You are a computer science major

f = You are a freshman

only if = \rightarrow

or = \vee

$a \rightarrow (c \vee \neg f)$.

Example: "You cannot ride the roller coaster if you are under 4 feet tall unless you are older than 16 years old."

Translate this sentence into a logical expression.

Example: "You cannot ride the roller coaster if you are under 4 feet tall unless you are older than 16 years old."

Translate this sentence into a logical expression.

Solution:

q = You can ride the roller coaster.

r = You are under 4 feet tall

s = You are older than 16 years old.

$$(r \wedge \neg s) \rightarrow \neg q.$$

Mat2033 - Discrete Mathematics

Logic and Bit Operations

Computers represent information using bits. A bit has two possible values, namely, 0 and 1. This meaning of the word bit comes from binary digit, since zeros and ones are the digits used in binary representations of numbers.

A bit can be used to represent a truth value, since there are two truth values, namely, true and false. We will use a 1 bit to represent true and a 0 bit to represent false. That is, 1 represents T(true), 0 represents F(false). A variable is called a Boolean Variable if its value is either true or false.

Consequently, a Boolean Variable can be represented using a bit.

Computer bit operations correspond to the logical connectives. By replacing true by ' 1 ', and false by a ' 0 ', in the truth tables for the operators \wedge , \vee , and \oplus , the tables shown in below Table for the corresponding bit operations are obtained. We will also use the notation OR, AND, and XOR for the operators \vee , \wedge , and \oplus , as is done in various programming languages.

Information is often represented using bit strings, which are sequences of zeros and ones. When this is done, operations on the bit strings can be used to manipulate this information.

Information is often represented using bit strings, which are sequences of zeros and ones. When this is done, operations on the bit strings can be used to manipulate this information.

TABLE 7 : Tables for the bit operators OR, AND and XOR.

X	y
0	0
0	1
1	0
1	1

Information is often represented using bit strings, which are sequences of zeros and ones. When this is done, operations on the bit strings can be used to manipulate this information.

TABLE 7 : Tables for the bit operators OR, AND and XOR.

X	Y	X V Y
0	0	0
0	1	1
1	0	1
1	1	1

Information is often represented using bit strings, which are sequences of zeros and ones. When this is done, operations on the bit strings can be used to manipulate this information.

TABLE 7 : Tables for the bit operators OR, AND and XOR.

X	Y	XVY	XΛY
0	0	0	0
0	1	1	0
1	0	1	0
1	1	1	1

Information is often represented using bit strings, which are sequences of zeros and ones. When this is done, operations on the bit strings can be used to manipulate this information.

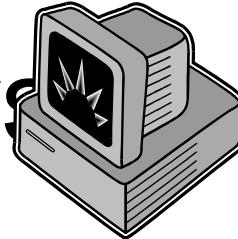
TABLE 7 : Tables for the bit operators OR, AND and XOR.

x	y	$x \vee y$	$x \wedge y$	$x \oplus y$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

Definition 7: A bit string is a sequence of zero or more bits. The length of this string is the number of bits in the string.

We can extend bit operations to bit strings. We define the bitwise OR, bitwise AND, and bitwise XOR of two strings of the same length to be the strings that have as their bits the OR, AND, and XOR of the corresponding bits in the two strings, respectively. We use the symbols \vee , \wedge , and \oplus to represent the bitwise OR, bitwise AND, and bitwise XOR operations, respectively.

Bitwise operators



$$\begin{array}{l} \text{a\&b AND } \wedge \\ \begin{array}{r r} 1101 & 1001 \\ 1110 & 0100 \\ \hline 1100 & 0000 \end{array} \end{array}$$

$$\begin{array}{l} \text{a|b OR } \vee \\ \begin{array}{r r} 1101 & 1001 \\ 1110 & 0100 \\ \hline 1111 & 1101 \end{array} \end{array}$$

$$\begin{array}{l} \text{a}^{\wedge} \text{b XOR } \oplus \\ \begin{array}{r r} 1101 & 1001 \\ 1110 & 0100 \\ \hline 0011 & 1101 \end{array} \end{array}$$

Example: Find the bitwise OR, bitwise AND, and bitwise XOR of the bit strings 011011 0110 and 110001 1101.

Solution:

Example: Find the bitwise OR, bitwise AND, and bitwise XOR of the bit strings 0110110110 and 1100011101.

Solution:

$$\begin{array}{r} 0110110110 \\ 1100011101 \\ \hline \end{array}$$

Example: Find the bitwise OR, bitwise AND, and bitwise XOR of the bit strings 0110110110 and 1100011101.

Solution:

$$\begin{array}{r} 0110110110 \\ 1100011101 \\ \hline 1110111101 \end{array}$$

bitwise OR

Example: Find the bitwise OR, bitwise AND, and bitwise XOR of the bit strings 0110110110 and 1100011101.

Solution:

$$\begin{array}{r} 0110110110 \\ 1100011101 \\ \hline \end{array}$$

0100010100 bitwise AND

Example: Find the bitwise OR, bitwise AND, and bitwise XOR of the bit strings 0110110110 and 1100011101.

Solution:

$$\begin{array}{r} 0110110110 \\ 1100011101 \\ \hline \end{array}$$

1010101111 bitwise XOR

Propositional Equivalences

Definition 1: A compound proposition that is always true, no matter what the truth values of the propositions that occur in it, is called a tautology. A compound proposition that is always false is called a contradiction. Finally, a proposition that is neither a tautology nor a contradiction is called a contingency. The following exp. illustrates these types of propositions.

Table 1 : Examples of Tautology and a Contradiction.			
P	$\neg P$	$P \vee \neg P$	$P \wedge \neg P$
T	F	T	F
F	T	T	F

Tautology

Tautology - a compound proposition that is always true.

$(p \rightarrow q) \vee p$	p	q	$p \rightarrow q$	$(p \rightarrow q) \vee p$
	T	T	T	T
	T	F	F	T
	F	T	T	T
	F	F	T	T

Contradiction

Contradiction - a compound proposition that is always false.

p	$\neg p$	$p \wedge \neg p$
T	F	F
F	T	F

Contingency

A **contingency** is neither a tautology nor a contradiction.

$$p \rightarrow (p \wedge q)$$

p	q	$p \wedge q$	$p \rightarrow (p \wedge q)$
T	T	T	T
T	F	F	F
F	T	F	T
F	F	F	T

Logical Equivalences

Compound propositions that have the same truth values in all possible cases are called logically equivalent

Definition 2: The propositions p and q are called logically equivalent if $p \leftrightarrow q$ is a tautology. The notation $p \leftrightarrow q$ denotes that p and q are logically equivalent.

Logical Equivalence

Compound propositions
that always have the same
truth value are called
logically equivalent.



Example: Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent.

Example: Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent.

Solution:

Table 2: Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$

p	q
T	T
T	F
F	T
F	F

Example: Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent.

Solution:

Table 2: Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Example: Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent.

Solution:

Table 2: Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$

p	q	$p \vee q$	$\neg(p \vee q)$
T	T	T	F
T	F	T	F
F	T	T	F
F	F	F	T

Example: Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent.

Solution:

Table 2: Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$
T	T	T	F	F
T	F	T	F	F
F	T	T	F	T
F	F	F	T	T

Example: Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent.

Solution:

Table 2: Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$
T	T	T	F	F	F
T	F	T	F	F	T
F	T	T	F	T	F
F	F	F	T	T	T

Example: Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent.

Solution:

Table 2: Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Example: Show that the propositions $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent.

Example: Show that the propositions $P \rightarrow q$ and $\neg P \vee q$ are logically equivalent.

Solution:

P	q	
T	T	
T	F	
F	T	
F	F	

Example: Show that the propositions $P \rightarrow q$ and $\neg P \vee q$ are logically equivalent.

Solution:

P	q	$\neg P$
T	T	F
T	F	F
F	T	T
F	F	T

Example: Show that the propositions $P \rightarrow q$ and $\neg P \vee q$ are logically equivalent.

Solution:

P	q	$\neg P$	$\neg P \vee q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

Example: Show that the propositions $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent.

Solution:

p	q	$\neg p$	$\neg p \vee q$	$p \rightarrow q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

- Note: If a compound proposition involves n propositions then 2^n rows are required.
- The following tables contains some important equivalences. In these equivalences, T denotes any proposition that is always true and F denotes any proposition that is always false

Logical Equivalences

$$p \wedge T \Leftrightarrow p$$

Identity laws

$$\mathbf{x*1 = x}$$

$$p \vee F \Leftrightarrow p$$

$$\mathbf{x+0 = x}$$

$$p \vee T \Leftrightarrow T$$

Domination laws

$$\mathbf{x*0 = 0}$$

$$p \wedge F \Leftrightarrow F$$

$$p \vee p \Leftrightarrow p$$

Idempotent laws

$$p \wedge p \Leftrightarrow p$$

$$\neg(\neg p) \Leftrightarrow p$$

Double negation law

$$\mathbf{-(-x) = x}$$

Logical Equivalences

$$p \vee q \Leftrightarrow q \vee p$$

Commutative
laws

$$\mathbf{x+y = y+x}$$

$$p \wedge q \Leftrightarrow q \wedge p$$

$$\mathbf{x^*y = y^*x}$$

$$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$$

Associative laws

$$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$$

$$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$$

Distributive laws

$$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$$

$$\neg(q \wedge r) \Leftrightarrow \neg q \vee \neg r$$

DeMorgan's laws

$$\neg(q \vee r) \Leftrightarrow \neg q \wedge \neg r$$

Logical Equivalences

$$p \vee \neg p \Leftrightarrow T$$

$$p \wedge \neg p \Leftrightarrow F$$

$$p \rightarrow q \Leftrightarrow (\neg p \vee q)$$

Note: that De Morgan's laws extend to

$$\neg(p_1 \vee p_2 \vee \dots \vee p_n) \iff (\neg p_1 \wedge \neg p_2 \wedge \dots \wedge \neg p_n)$$

and

$$\neg(p_1 \wedge p_2 \wedge \dots \wedge p_n) \iff (\neg p_1 \vee \neg p_2 \vee \dots \vee \neg p_n)$$

Example: Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent.

Example: Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent.

Solution:

$$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg(\neg p \wedge q) \quad 2. \text{ De Morgan's Law}$$

Example: Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent.

Solution:

$$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg(\neg p \wedge q) \quad 2. \text{ De Morgan's Law}$$

$$\Leftrightarrow \neg p \wedge [\neg(\neg p) \vee \neg q] \quad 1. \text{ De Morgan's Law}$$

Example: Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent.

Solution:

$$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg(\neg p \wedge q) \quad 2. \text{ De Morgan's Law}$$

$$\Leftrightarrow \neg p \wedge [\neg(\neg p) \vee \neg q] \quad 1. \text{ De Morgan's Law}$$

$$\Leftrightarrow \neg p \wedge (p \vee \neg q) \quad \text{Double Negation Law}$$

Example: Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent.

Solution:

$$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg(\neg p \wedge q) \quad 2. \text{ De Morgan's Law}$$

$$\Leftrightarrow \neg p \wedge [\neg(\neg p) \vee \neg q] \quad 1. \text{ De Morgan's Law}$$

$$\Leftrightarrow \neg p \wedge (p \vee \neg q) \quad \text{Double Negation Law}$$

$$\Leftrightarrow (\neg p \wedge p) \vee (\neg p \wedge \neg q) \quad \text{Distributive Law}$$

Example: Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent.

Solution:

$$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg(\neg p \wedge q) \quad 2. \text{ De Morgan's Law}$$

$$\Leftrightarrow \neg p \wedge [\neg(\neg p) \vee \neg q] \quad 1. \text{ De Morgan's Law}$$

$$\Leftrightarrow \neg p \wedge (p \vee \neg q) \quad \text{Double Negation Law}$$

$$\Leftrightarrow (\neg p \wedge p) \vee (\neg p \wedge \neg q) \quad \text{Distributive Law}$$

$$\Leftrightarrow F \vee (\neg p \wedge \neg q) \quad \text{since } \neg p \wedge p \Leftrightarrow F$$

Example: Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent.

Solution:

$$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg(\neg p \wedge q) \quad 2. \text{ De Morgan's Law}$$

$$\Leftrightarrow \neg p \wedge [\neg(\neg p) \vee \neg q] \quad 1. \text{ De Morgan's Law}$$

$$\Leftrightarrow \neg p \wedge (p \vee \neg q) \quad \text{Double Negation Law}$$

$$\Leftrightarrow (\neg p \wedge p) \vee (\neg p \wedge \neg q) \quad \text{Distributive Law}$$

$$\Leftrightarrow F \vee (\neg p \wedge \neg q) \quad \text{since } \neg p \wedge p \Leftrightarrow F$$

$$\Leftrightarrow (\neg p \wedge \neg q) \vee F \quad \text{Law of disjunction}$$

$$\Leftrightarrow \neg p \wedge \neg q \quad \text{Identity Law}$$

Example: Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

Example: Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

Solution:

$$(p \wedge q) \rightarrow (p \vee q) \iff \neg(p \wedge q) \vee (p \vee q)$$

Example: Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

Solution:

$$\begin{aligned}(p \wedge q) \rightarrow (p \vee q) &\iff \neg(p \wedge q) \vee (p \vee q) \\ &\iff (\neg p \vee \neg q) \vee (p \vee q) \text{ 1. De Morgan's Law}\end{aligned}$$

Example: Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

Solution:

$$(p \wedge q) \rightarrow (p \vee q) \iff \neg(p \wedge q) \vee (p \vee q)$$

$$\iff (\neg p \vee \neg q) \vee (p \vee q) \text{ 1. De Morgan's Law}$$

$$\iff (\neg p \vee p) \vee (\neg q \vee q) \text{ associative and commutative laws for disjunction}$$

Example: Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

Solution:

$$(p \wedge q) \rightarrow (p \vee q) \iff \neg(p \wedge q) \vee (p \vee q)$$

$$\iff (\neg p \vee \neg q) \vee (p \vee q) \quad \text{1. De Morgan's Law}$$

$$\iff (\neg p \vee p) \vee (\neg q \vee q) \quad \begin{array}{l} \text{associative and} \\ \text{commutative laws for} \\ \text{disjunction} \end{array}$$

$$\iff T \vee T$$

$$\iff T \quad \text{Domination Law}$$

Implication

$$p \rightarrow q$$

- “if p, then q”
- “p implies q”
- “if p,q”
- “p only if q”
- “p is sufficient for q”
- “q if p”
- “q whenever p”
- “q is necessary for p”
- “q when p”
- “a necessary condition for p is q”
- “a sufficient condition for q is p”
- “q follows from p”
- “q, it is sufficient that p”
- “q, it is sufficient to p”
- “p, it is necessary that q”
- “it is necessary to q, p”

Example

Express these system specifications using the propositions p “The message is scanned for viruses” and q “The message was sent from an unknown system” together with logical connectives.

- a) “The message is scanned for viruses whenever the message was sent from an unknown system.”
- b) “The message was sent from an unknown system but it was not scanned for viruses.”
- c) “It is necessary to scan the message for viruses whenever it was sent from an unknown system.”
- d) “When a message is not sent from an unknown system it is not scanned for viruses.”

Example

Express these system specifications using the propositions p “The message is scanned for viruses” and q “The message was sent from an unknown system” together with logical connectives.

- a) “The message is scanned for viruses whenever the message was sent from an unknown system.” a) $q \rightarrow p$
- b) “The message was sent from an unknown system but it was not scanned for viruses.” b) $q \wedge \neg p$
- c) “It is necessary to scan the message for viruses whenever it was sent from an unknown system.” c) $q \rightarrow p$
- d) “When a message is not sent from an unknown system it is not scanned for viruses.” d) $\neg q \rightarrow \neg p$

Mat2033 - Discrete Mathematics

The Foundations: Logic and Proof, Sets and Functions

Section 1.3 - 1.4

Predicates & Quantifiers



Predicates and Quantifiers

Statements involving variables, such as

" $x > 3$ ", " $x = y + 3$ ", and " $x + y = z$ "

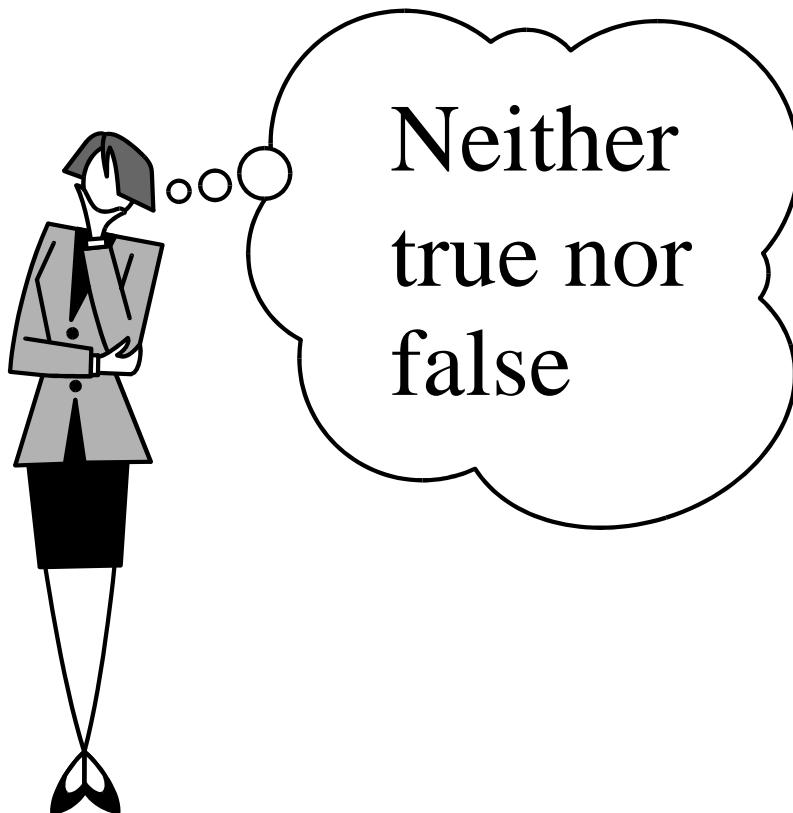
are often found in mathematical assertions and in computer programs. These statements are neither true nor false when the values of the variables are not specified. The statement " x is greater than 3" has two parts. The first part, the variable x , is the subject of the statement. The second part - the predicate, "is greater than 3" — refers to a property that the subject of the statement can have. We can denote the statement " x is greater than 3" by $P(x)$, where P denotes the predicate "is greater than 3" and x is the variable. The statement $P(x)$ is also said to be the value of the propositional

Open Statement

$x > 8$

$p < q - 5$

$x = y + 6$



Propositional Functions

$x > 8$

x is greater than 8.

x is greater than 8.

subject predicate

Propositional Functions

x is greater than 8.

subject predicate

$P(x)$

propositional function P
at x

Propositional Functions

There are two ways a propositional function

$$P(x) \quad "x > 8"$$

can become true or false (a proposition)

P (x) “x > 8”

1. The variable may be given a value

P (5) “5 > 8” **FALSE**

P (12) “12 > 8” **TRUE**

Propositional Functions (two variables)

Let $Q(x, y)$ be the statement
“ x is the capital of y . ”

What are the truth values of:

$Q(\text{Paris}, \text{France})$

$Q(\text{Ankara}, \text{Greece})$

Example: Let $P(x)$ denote the statement " $x > 3$ ". What are the truth values of $P(4)$ and $P(2)$?

Example: Let $P(x)$ denote the statement " $x > 3$ ". What are the truth values of $P(4)$ and $P(2)$?

Solution: $P(4)$ means " $4 > 3$ " (True)

Example: Let $P(x)$ denote the statement " $x > 3$ ". What are the truth values of $P(4)$ and $P(2)$?

Solution: $P(4)$ means " $4 > 3$ " (True)

$P(2)$ means " $2 > 3$ " (False)

Example: Let $P(x)$ denote the statement " $x > 3$ ". What are the truth values of $P(4)$ and $P(2)$?

Solution: $P(4)$ means " $4 > 3$ " (True)

$P(2)$ means " $2 > 3$ " (False)

Example: Let $Q(x,y)$ denote the statement " $x = y + 3$ ". What are the truth values of the propositions $Q(1,2)$ and $Q(3,0)$?

Example: Let $P(x)$ denote the statement " $x > 3$ ". What are the truth values of $P(4)$ and $P(2)$?

Solution: $P(4)$ means " $4 > 3$ " (True)

$P(2)$ means " $2 > 3$ " (False)

Example: Let $Q(x,y)$ denote the statement " $x = y + 3$ ". What are the truth values of the propositions $Q(1,2)$ and $Q(3,0)$?

Solution:

$Q(1,2)$ means " $1 = 2 + 3$ " which is False.

Example: Let $P(x)$ denote the statement " $x > 3$ ". What are the truth values of $P(4)$ and $P(2)$?

Solution: $P(4)$ means " $4 > 3$ " (True)

$P(2)$ means " $2 > 3$ " (False)

Example: Let $Q(x,y)$ denote the statement " $x = y + 3$ ". What are the truth values of the propositions $Q(1,2)$ and $Q(3,0)$?

Solution:

$Q(1,2)$ means " $1 = 2 + 3$ " which is False.

$Q(3,0)$ means " $3 = 0 + 3$ " which is True.

Example: Let $R(x,y,z)$ denote the statement " $x+y=z$ ". What are the truth values of the propositions $R(1,2,3)$ and $R(0,0,1)$?

Example: Let $R(x,y,z)$ denote the statement " $x+y=z$ ". What are the truth values of the propositions $R(1,2,3)$ and $R(0,0,1)$?

Solution :

$R(1,2,3)$ means " $1+2=3$ " which is True.

$R(0,0,1)$ means " $0+0=1$ " which is False. ▀

In general, a statement involving the n variables x_1, x_2, \dots, x_n can be denoted by

$$P(x_1, x_2, \dots, x_n).$$

A statement of the form $P(x_1, x_2, \dots, x_n)$ is the value of the propositional function P . at the n -tuple (x_1, x_2, \dots, x_n) , and P is also called a predicate.

Quantifiers

2. A propositional function

$P(x)$ “ $x > 8$ ”

can become true or false (a proposition) by using
quantifiers.

Quantifiers

When all the variables in a propositional function are assigned values, the resulting statement has a truth value. However, there is another important way, called quantification to create a proposition from a propositional function. Two types of quantification will be discussed here, namely, universal quantification and existential quantification.

Many mathematical statements assert that a property is true for all values of a variable in a particular domain, called the universe of discourse. Such a statement is expressed using a universal quantification. The universal quantification of a propositional function is the proposition that asserts that $P(x)$ is true for all values of x in the universe of discourse.

Universal Quantification

A Universal Quantifier states that $P(x)$ is true for all values of x in the universe of discourse.

$$\forall x P(x)$$



states the universal quantification of
 $P(x)$

Here \forall is called the universal quantifier. The proposition $\forall x P(x)$ is also expressed as

"for all $x P(x)$ " or "for every $x P(x)$ "

Example: Express the statement

"Every student in this class has studied calculus"

as a universal quantification.

Example: Express the statement

"Every student in this class has studied calculus"

as a universal quantification.

Solution: Let $P(x)$ denote the statement

" x has studied calculus"

Example: Express the statement

"Every student in this class has studied calculus"

as a universal quantification.

Solution: Let $P(x)$ denote the statement

" x has studied calculus"

Then the statement "Every student in this class has studied calculus" can be written as $\forall x P(x)$, where the universe of discourse consists of the students in this class.

Example: Let $P(x)$ be the statement " $x+1 > x$ ". What is the truth value of the quantification $\forall x P(x)$, where the universe of discourse is the set of real numbers?

Example: Let $P(x)$ be the statement " $x+1 > x$ ". What is the truth value of the quantification $\forall x P(x)$, where the universe of discourse is the set of real numbers?

Solution: Since $P(x)$ is true for all real numbers x , the quantification

$$\forall x P(x)$$

is true.

Example: Let $Q(x)$ be the statement " $x < 2$ ". What is the truth value of the quantification $\forall x Q(x)$, where the universe of discourse is the set of real numbers?

Example: Let $Q(x)$ be the statement " $x < 2$ ". What is the truth value of the quantification $\forall x Q(x)$, where the universe of discourse is the set of real numbers?

Solution: $Q(x)$ is not true for all real numbers x , since, for instance, $Q(3)$ is false. Thus

$$\forall x Q(x)$$

is false.

Note: When all the elements in the universe of discourse can be listed - say, x_1, x_2, \dots, x_n - it follows that the universal quantification $\forall x P(x)$ is the same as the conjunction

$$P(x_1) \wedge P(x_2) \wedge \dots \wedge P(x_n)$$

Since this conjunction is true if and only if $P(x_1), P(x_2), \dots, P(x_n)$ are all true.

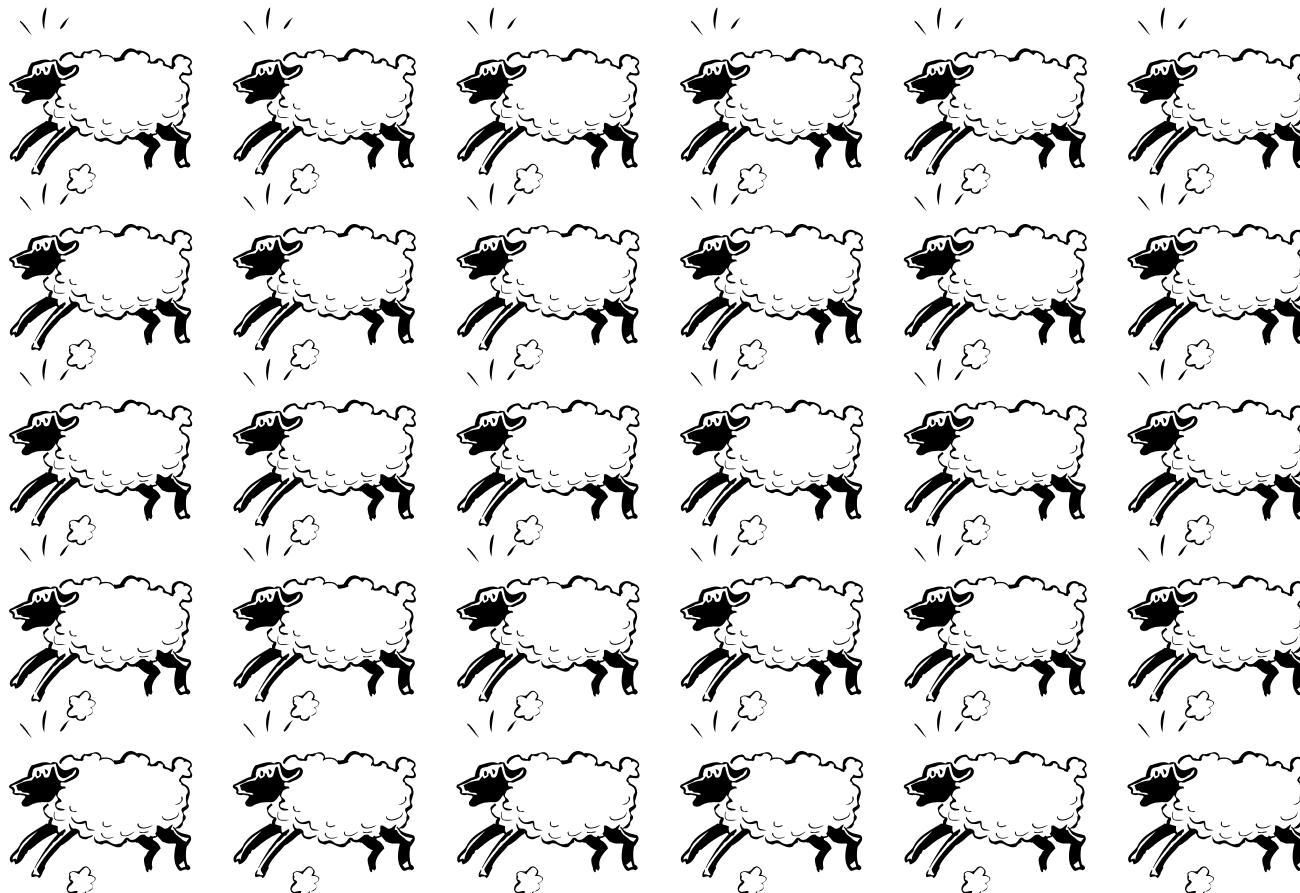
Example: $P(n)$ is the statement " $x^2 < 10$ ", where the universe of discourse is the positive integers not exceeding 4. What is the truth value of $\forall x P(x)$?

Example: $P(n)$ is the statement " $x^2 < 10$ ", where the universe of discourse is the positive integers not exceeding 4. What is the truth value of $\forall x P(x)$?

Solution: $\forall x P(x)$ is true if $P(1) \wedge P(2) \wedge P(3) \wedge P(4)$ is true. $P(1)$, $P(2)$ and $P(3)$ are true but $P(4)$ is not true. So $\forall x P(x)$ is False.

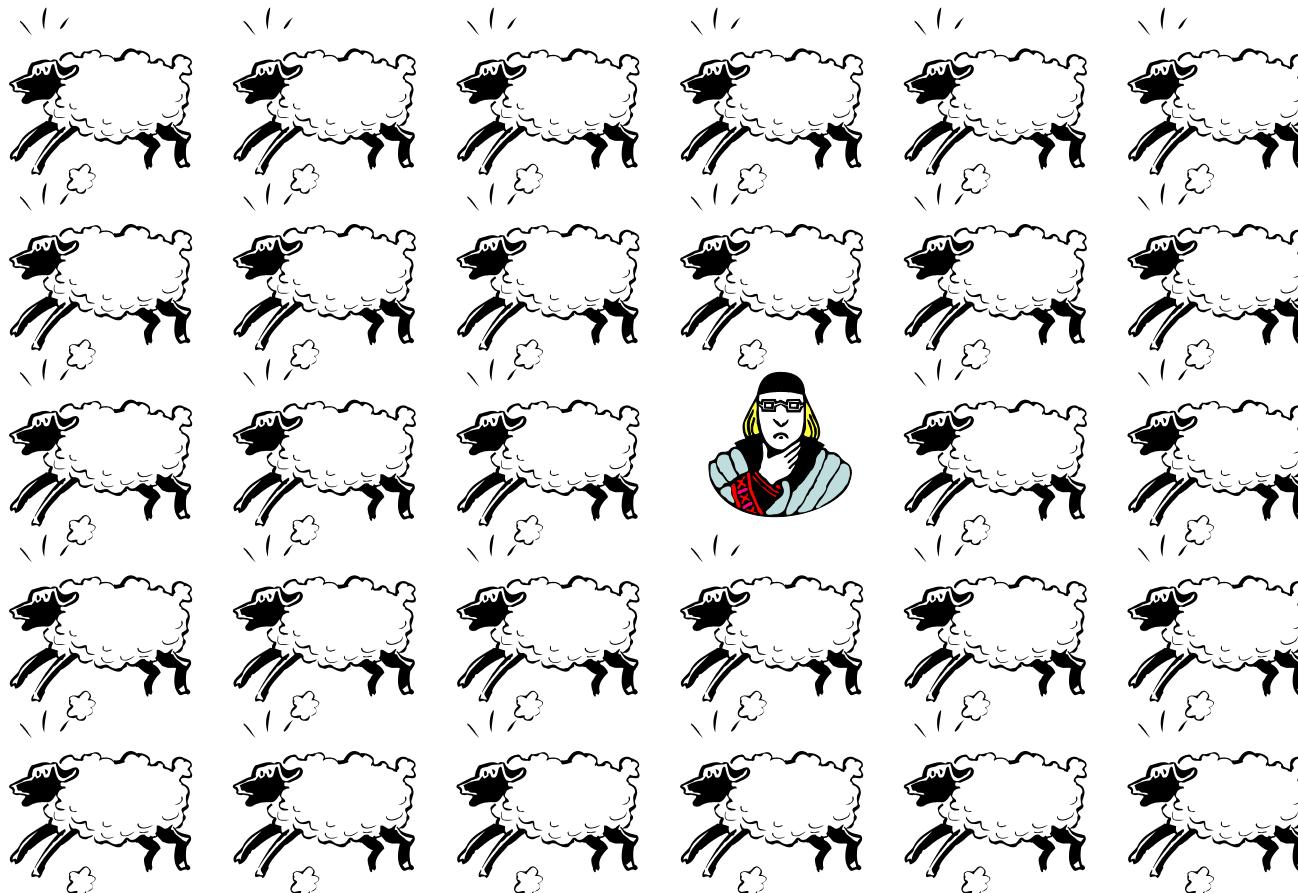
$\forall x P(x)$

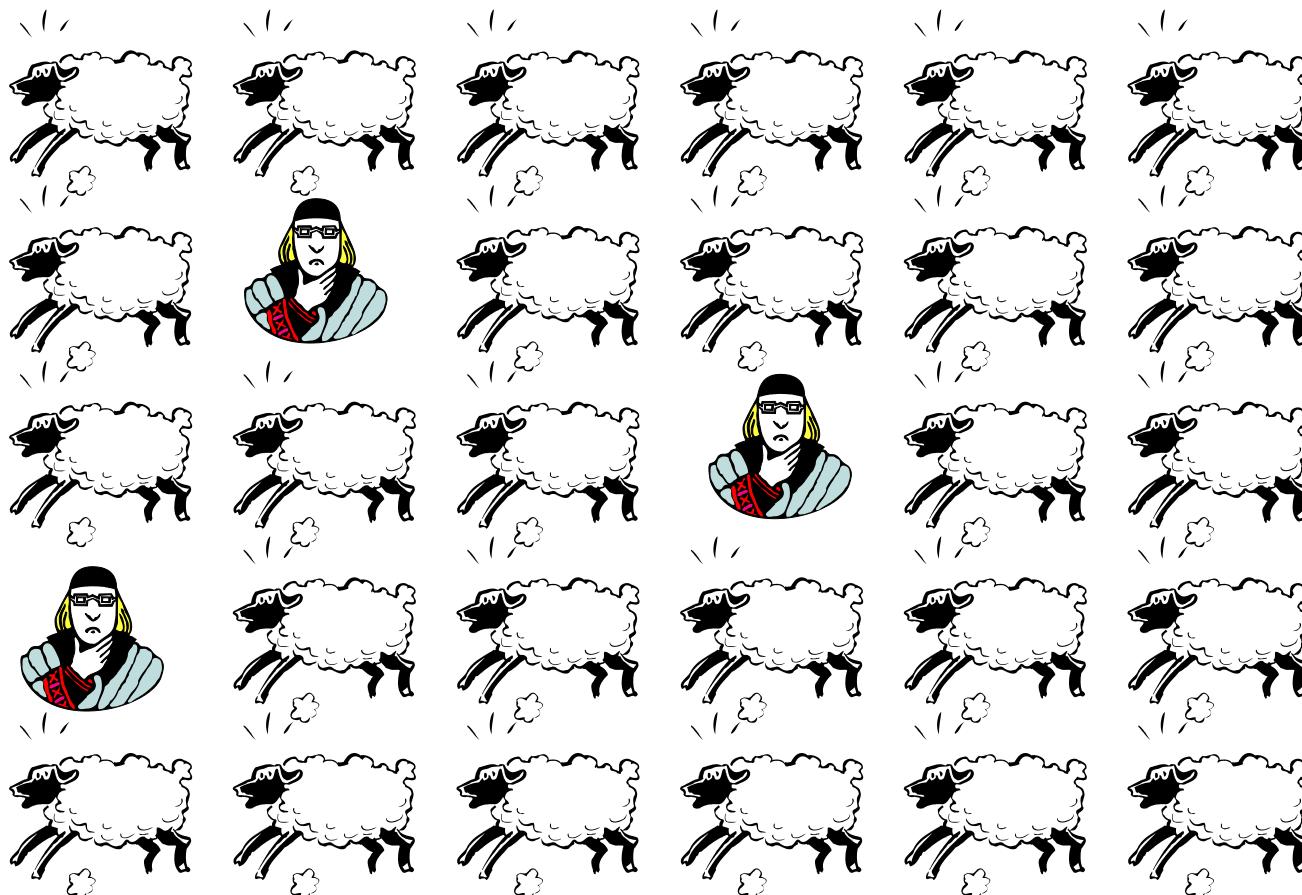
True



$$\forall x P(x)$$

False



$\forall x P(x)$ False

$$\forall x P(x)$$

False



Universal Quantification

Example: Every person in this class has completed MATH 2033.

Let $P(x)$ represent the statement “ x has completed MATH 2033” where the universe of discourse is this class.

$$\forall x P(x)$$

then represents the above statement.

If $S(x)$ represented the statement “x is in this class” and

$P(x)$ denotes the statement “x has had MATH 2033”

or its equivalent

$$\forall x(S(x) \rightarrow P(x))$$

Also represents the statement.

Universe of Discourse



It is important to note that the universe of discourse must be defined before the logical value of a propositional function may be discussed.

Example:



Let $P(x)$ be the statement “ x spends more than five hours every weekday in class,” where the universe of discourse for x is the set of students. Express $\forall x \neg P(x)$ in English.

No student spends more than five hours every weekday in class

Existential Quantification

States that $P(x)$ is true for *some* value of x in the universe of discourse.

$$\exists x P(x)$$



states the existential quantification of
 $P(x)$

Definition 2: The existential quantification of $P(x)$ is the proposition

"There exists an element x in the universe of discourse such that $P(x)$ is true"

We use the notation

$$\exists x P(x)$$

for the existential quantification of $P(x)$. Here \exists is called the existential quantifier. The existential quantification $\exists x P(x)$ is also expressed as

"There is an x such that $P(x)$ "

"There is at least one x such that $P(x)$ "

or

"For some $x P(x)$ ".

Example: Let $P(x)$ denote the statement " $x > 3$ ". What is the truth value of the quantification $\exists x P(x)$, where the universe of discourse is the set of real numbers?

Example: Let $P(x)$ denote the statement " $x > 3$ ". What is the truth value of the quantification $\exists x P(x)$, where the universe of discourse is the set of real numbers?

Solution: Since " $x > 3$ " is true - for instance, when $x=4$ - the existential quantification of $P(x)$, which is $\exists x P(x)$, is true.

Existential Quantification

There is at least one person in this class who has completed MATH 2033.

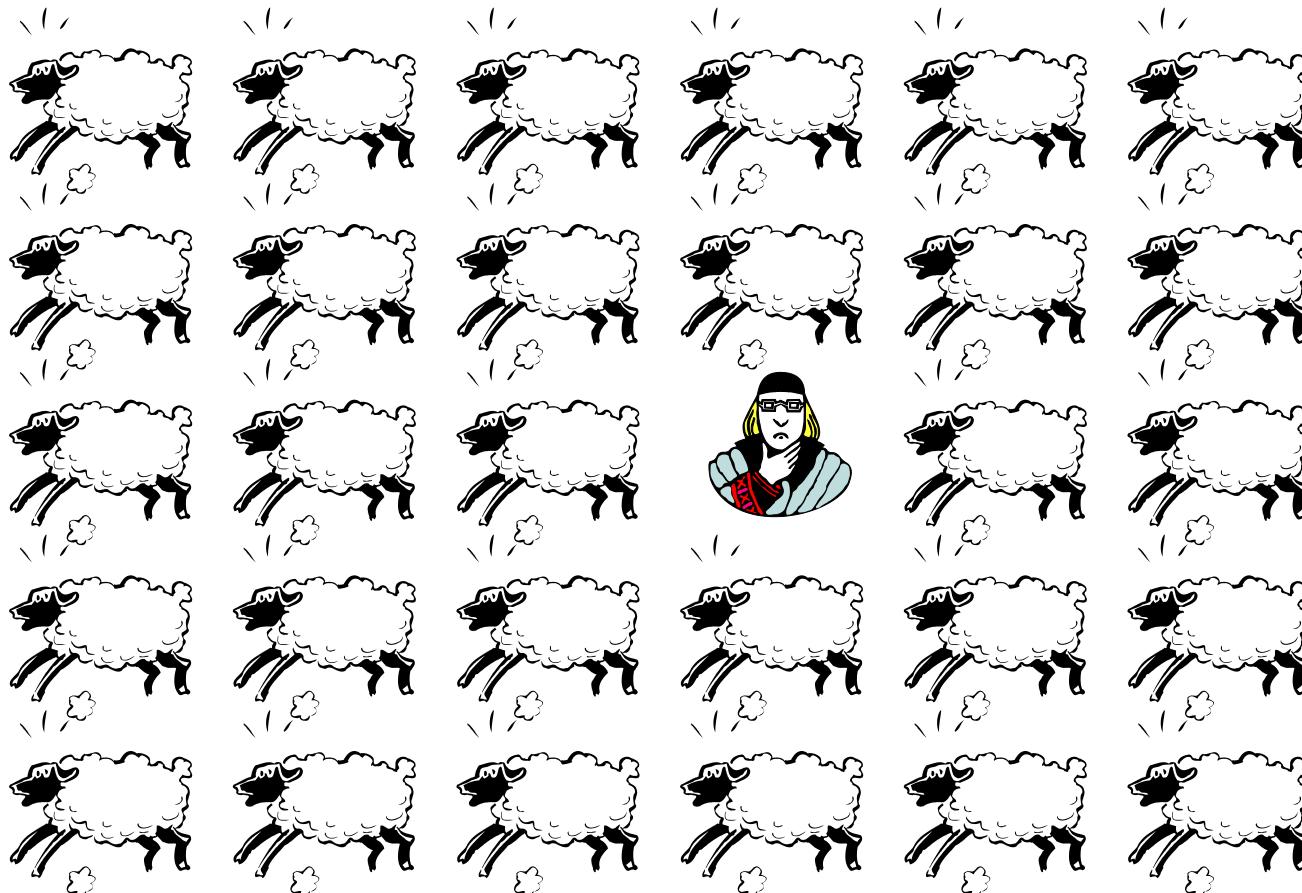
Let $P(x)$ represent the statement “ x has completed MATH 2033” where the universe of discourse is this class.

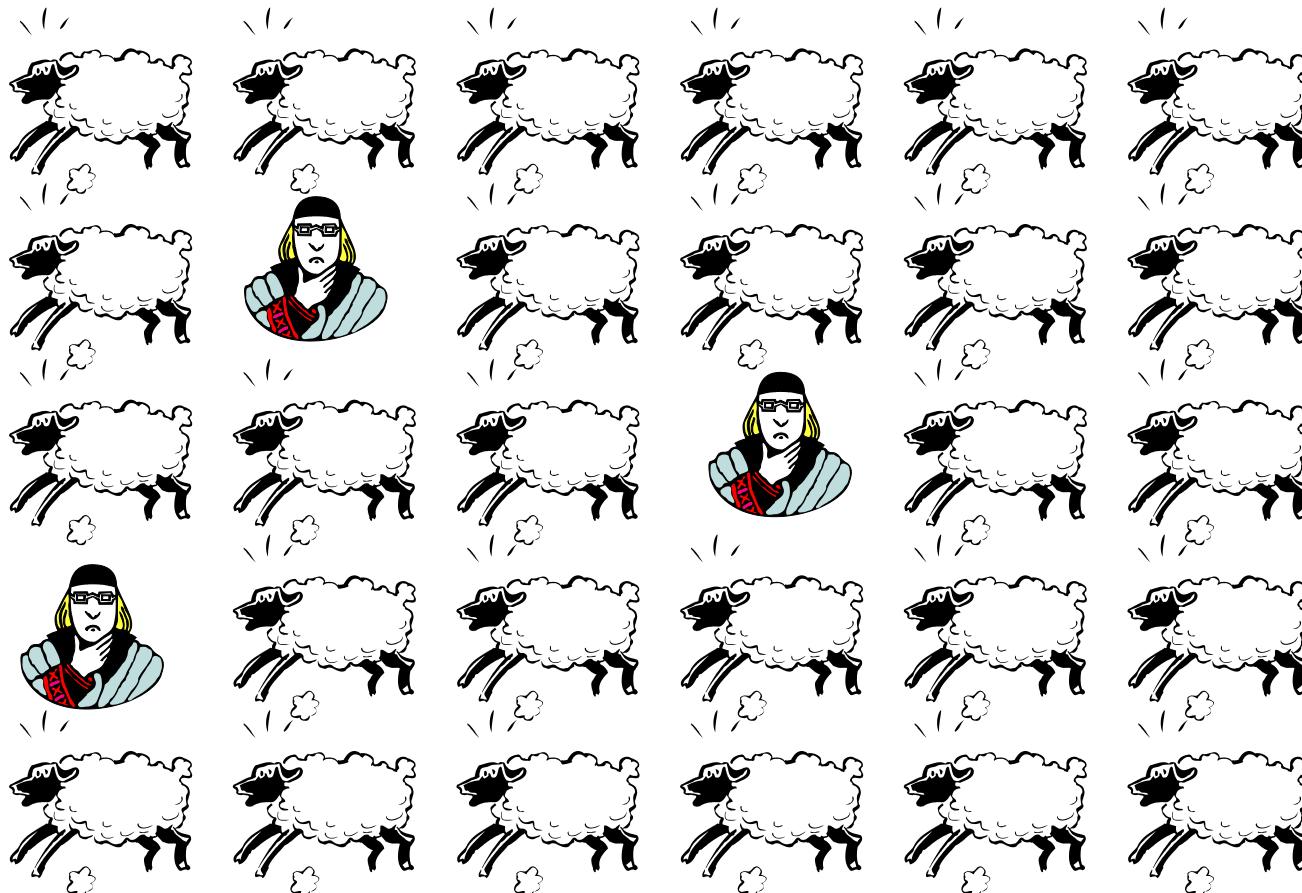
$$\exists x P(x)$$

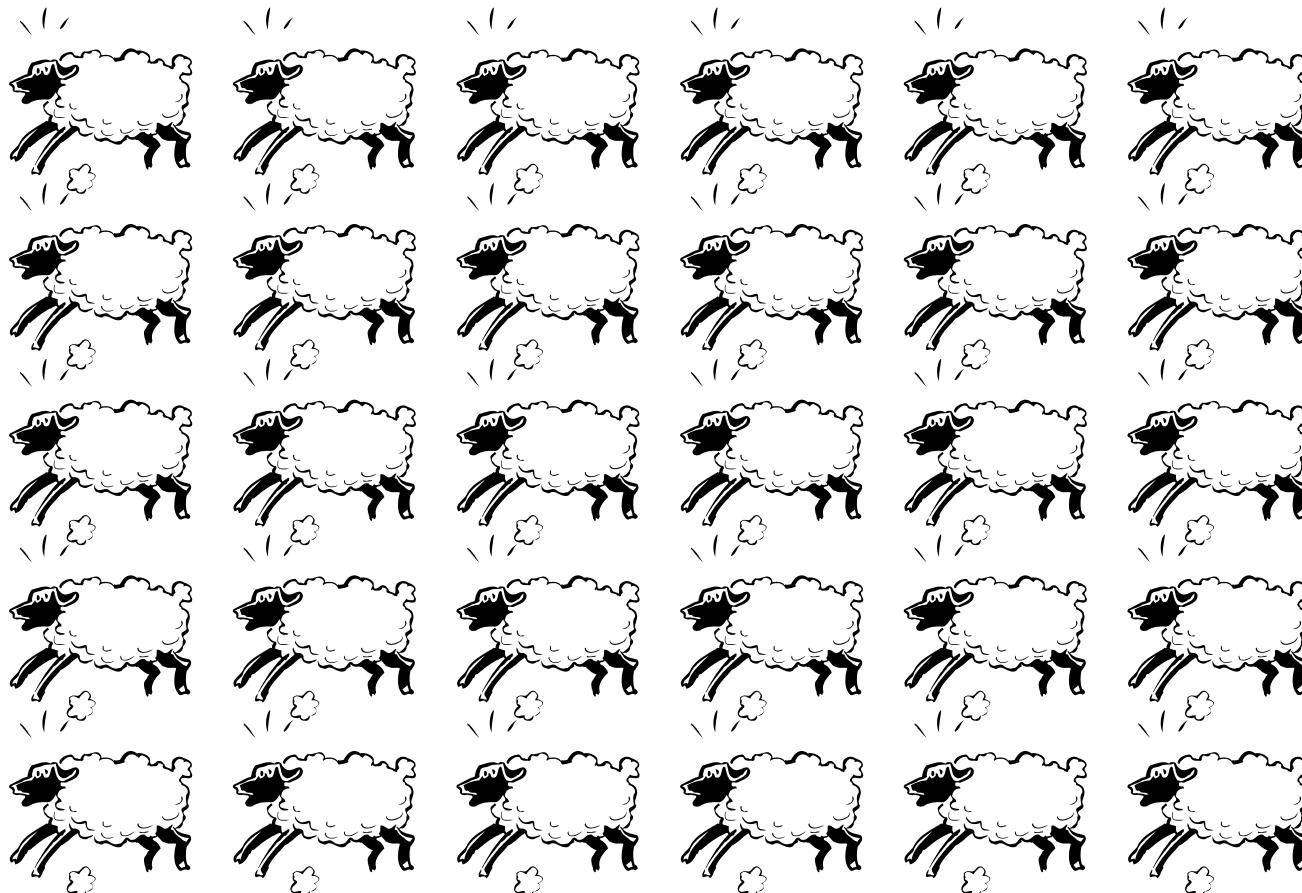
then represents the above statement.

$\exists x P(x)$

True



$\exists x P(x)$ True

$\exists x P(x)$ False

$$\exists x P(x)$$

True



Example: Let $Q(x)$ denote the statement " $x = x+1$ ".

What is the truth value of the quantification $\exists x Q(x)$,
where the universe of discourse is the set of real numbers?

Example: Let $Q(x)$ denote the statement " $x = x+1$ ".

What is the truth value of the quantification $\exists x Q(x)$, where the universe of discourse is the set of real numbers?

Solution: $Q(x)$ is false for every number x , the existential quantification of $Q(x)$, which is $\exists x Q(x)$, is false.

Note: When all of the elements in the universe of discourse can be listed — say, x_1, x_2, \dots, x_n — the existential quantification $\exists x P(x)$ is the same as the disjunction

$$P(x_1) \vee P(x_2) \vee \dots \vee P(x_n)$$

since this disjunction is true if and only if at least one of $P(x_1), P(x_2), \dots, P(x_n)$ is true.

Example: What is the truth value of $\exists x P(x)$ where $P(x)$ is the statement " $x^2 > 10$ " and the universe of discourse consists of the positive integers not exceeding 4?

Example: What is the truth value of $\exists x P(x)$ where $P(x)$ is the statement " $x^2 > 10$ " and the universe of discourse consists of the positive integers not exceeding 4?

Solution: Since the universe of discourse is $\{1, 2, 3, 4\}$, the proposition $\exists x P(x)$ is the same as the disjunction

$$P(1) \vee P(2) \vee P(3) \vee P(4)$$

Since $P(4)$, which is the statement " $4^2 > 10$ " is true, it follows that $\exists x P(x)$ is true.

Example:

Let $P(x)$ be the statement “ x spends more than five hours every weekday in class,” where the universe of discourse for x is the set of students. Express $\exists x \neg P(x)$ in English.

There is some student (maybe more than one) who does not spend more than five hours every weekday in class.

Quantifiers

	TRUE	FALSE
$\forall x P(x)$	$P(x)$ must be true for every x .	There is some x for which $P(x)$ is false
$\exists x P(x)$	There is some x for which $P(x)$ is true.	$P(x)$ must be false for every x .

Example: Assume that the universe of discourse for the variables x and y is the set of all real numbers. The statement

$$\forall x \forall y (x+y = y+x)$$

says that $x+y = y+x$ for all real numbers x and y . This is the commutative Law for addition of real numbers.

Example: Assume that the universe of discourse for the variables x and y is the set of all real numbers. The statement

$$\forall x \forall y (x+y = y+x)$$

says that $x+y = y+x$ for all real numbers x and y . This is the commutative Law for addition of real numbers.

* $\forall x \exists y (x+y=0)$

Says that for every real number x there is a real number y such that $x+y=0$. This states that every real number has an additive inverse.

Example: Assume that the universe of discourse for the variables x and y is the set of all real numbers. The statement

$$\forall x \forall y (x+y = y+x)$$

says that $x+y = y+x$ for all real numbers x and y . This is the commutative Law for addition of real numbers.

* $\forall x \exists y (x+y=0)$

Says that for every real number x there is a real number y such that $x+y=0$. This states that every real number has an additive inverse.

* $\forall x \forall y \forall z (x+(y+z) = (x+y)+z)$

is the associative law for addition of real numbers.

Many mathematical statements involve multiple quantifications of propositional functions involving more than one variable. It is important to note that the order of the quantifiers is important, unless all the quantifiers are universal quantifiers or all are existential quantifiers.

Quantifiers with Multiple Variables

$$\forall x \forall y P(x, y)$$

$$\forall y \forall x P(x, y)$$

Multiple Variables

$$\exists x \exists y P(x, y)$$

$$\exists y \exists x P(x, y)$$

Multiple Variables

$$\exists x \forall y P(x, y)$$

$$\forall y \exists x P(x, y)$$

$$\exists y \forall x P(x, y)$$

$$\forall x \exists y P(x, y)$$

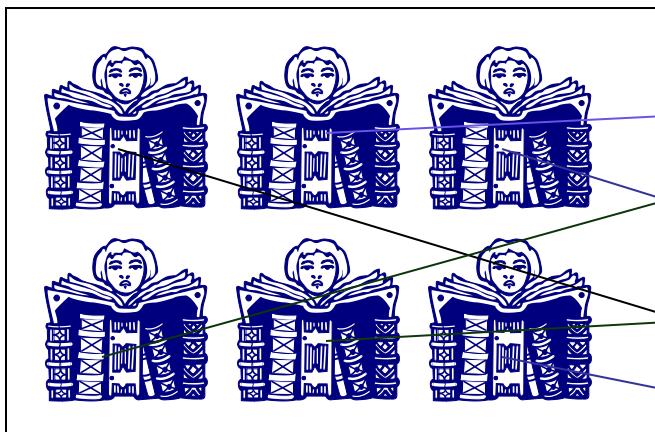
Take care in
reading these.

Example:

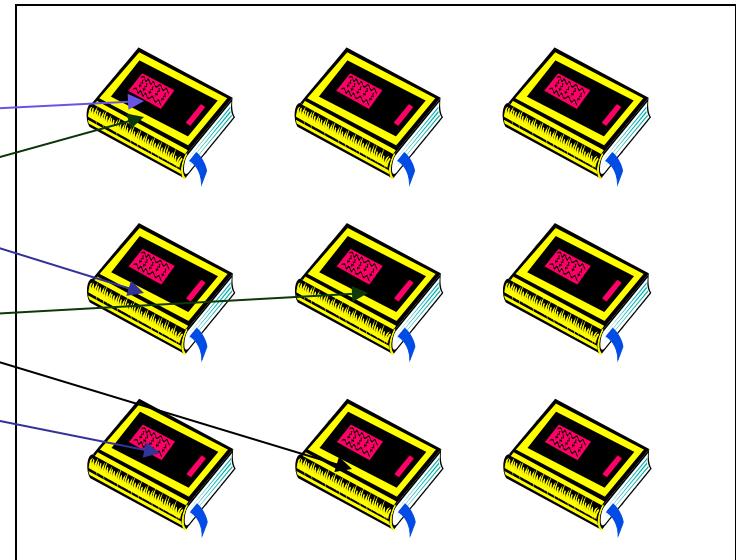
Let $P(x, y)$ be the statement “ x has taken class y ,” where the universe of discourse for x is the set of all students in this class and for y is the set of all MATH courses at the University.

$$\forall x \exists y P(x, y)$$

For every student in this class, there is a MATH course that student has taken.



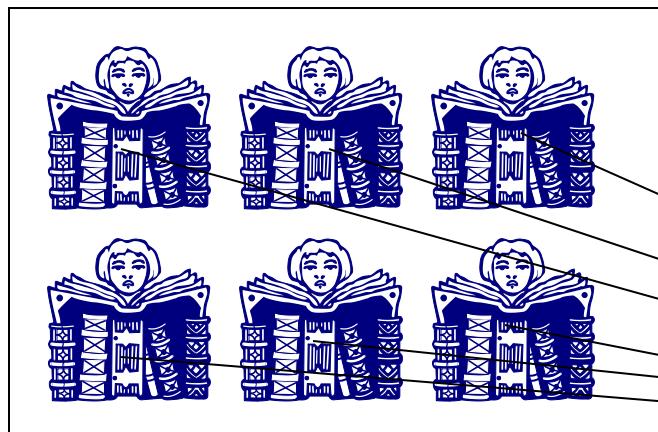
Students in this class



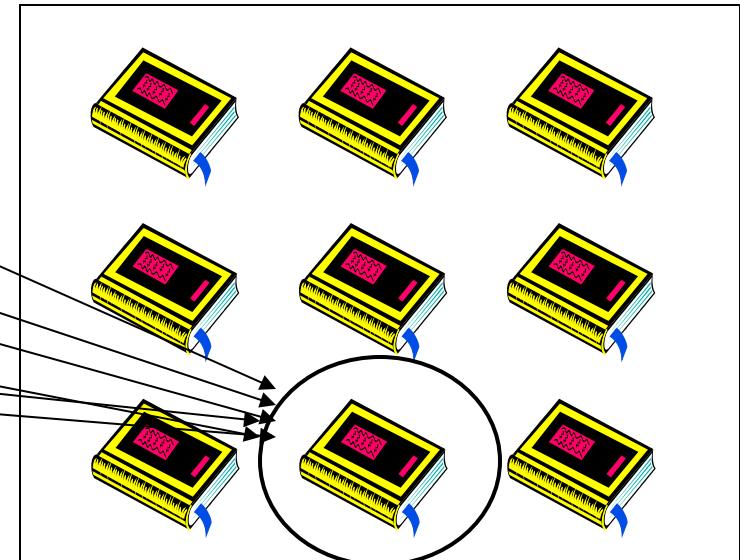
MATH Courses

$$\exists y \forall x P(x, y)$$

There is a MATH course that every student in this class has taken.



Students in this class

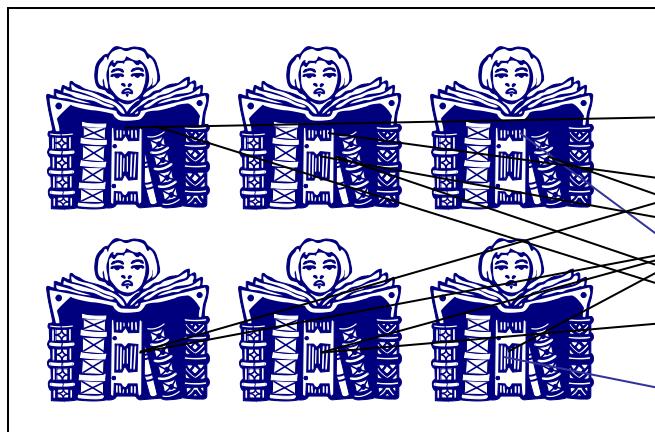


Example:

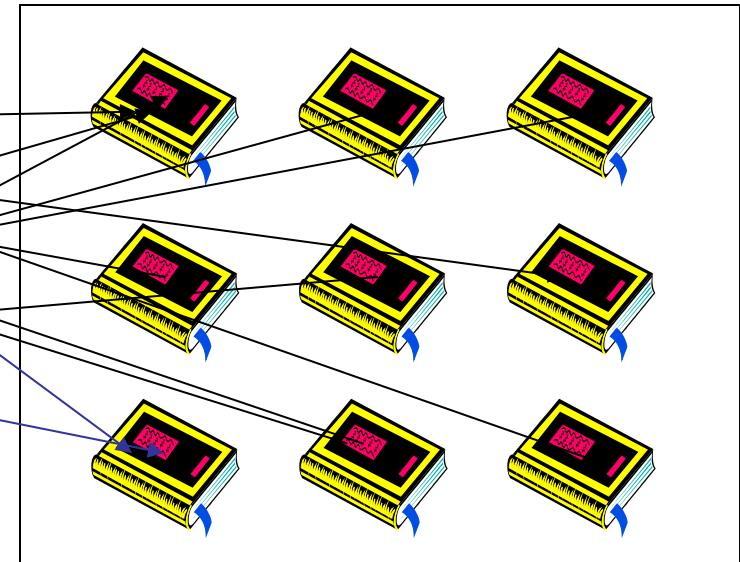
Let $P(x, y)$ be the statement “ x has taken class y ,” where the universe of discourse for x is the set of all students in this class and for y is the set of all MATH courses at the University.

$$\forall y \exists x P(x, y)$$

For every (pick any one you want) MATH course, there is a student in this class who has taken the course.



Students in this class



Example: Translate the statement

$$\forall x \{ C(x) \vee \exists y [C(y) \wedge F(x,y)] \}$$

into English, where $C(x)$ is "x has a computer" $F(x,y)$ is "x and y are friends," and the universe of discourse for both x and y is the set of all students in your school.

Example: Translate the statement

$$\forall x \{ C(x) \vee \exists y [C(y) \wedge F(x,y)] \}$$

into English, where $C(x)$ is "x has a computer" $F(x,y)$ is "x and y are friends," and the universe of discourse for both x and y is the set of all students in your school.

Solution:

* For every student x in your school x has a computer or there is a student y such that y has a computer and x and y are friends.

Example: Translate the statement

$$\forall x \{ C(x) \vee \exists y [C(y) \wedge F(x,y)] \}$$

into English, where $C(x)$ is "x has a computer" $F(x,y)$ is "x and y are friends," and the universe of discourse for both x and y is the set of all students in your school.

Solution:

- * For every student x in your school x has a computer or there is a student y such that y has a computer and x and y are friends.
or
- * Every student in your school has a computer or has a friend who has a computer.

Example: Translate the statement

$$\exists x \forall y \forall z \{ [(F(x,y) \wedge F(x,z)) \wedge (y \neq z)] \rightarrow \neg F(y,z) \}$$

into English, where $F(a,b)$ means a and b are friends and the universe of discourse for x, y and z is the set of all students in your school.

Example: Translate the statement

$$\exists x \forall y \forall z \{ [(F(x,y) \wedge F(x,z)) \wedge (y \neq z)] \rightarrow \neg F(y,z) \}$$

into English, where $F(a,b)$ means a and b are friends and the universe of discourse for x, y and z is the set of all students in your school.

solution:

- * There is a student x such that for all students y and all students z other than y , if x and y are friends and x and z are friends, then y and z are not friends.

Example: Translate the statement

$$\exists x \forall y \forall z \{ [(F(x,y) \wedge F(x,z)) \wedge (y \neq z)] \rightarrow \neg F(y,z) \}$$

into English, where $F(a,b)$ means a and b are friends and the universe of discourse for x, y and z is the set of all students in your school.

solution:

- * There is a student x such that for all students y and all students z other than y , if x and y are friends and x and z are friends, then y and z are not friends.
- * In other words, there is a student none of whose friends are also friends with each other.

Translating Sentences into Logical Expressions:

Example: Express the statements

- i) "Some students in this class has visited Mexico"
- ii) "Every student in this class has visited either Canada or Mexico"

Using quantifiers-

Translating Sentences into Logical Expressions:

Example: Express the statements

- i) "Some students in this class has visited Mexico"
- ii) "Every student in this class has visited either Canada or Mexico"

Using quantifiers.

Solution: Let the universe of discourse for the variable x be the set of students in your class.

$M(x) \equiv x \text{ has visited Mexico.}$

$C(x) \equiv x \text{ has visited Canada.}$

Translating Sentences into Logical Expressions:

Example: Express the statements

- i) "Some students in this class has visited Mexico"
- ii) "Every student in this class has visited either Canada or Mexico"

Using quantifiers.

Solution: Let the universe of discourse for the variable x be the set of students in your class.

$M(x) \equiv x \text{ has visited Mexico.}$

$C(x) \equiv x \text{ has visited Canada.}$

i) $\exists x M(x)$

Translating Sentences into Logical Expressions:

Example: Express the statements

- i) "Some students in this class has visited Mexico"
- ii) "Every student in this class has visited either Canada or Mexico"

Using quantifiers.

Solution: Let the universe of discourse for the variable x be the set of students in your class.

$M(x) \equiv x \text{ has visited Mexico.}$

$C(x) \equiv x \text{ has visited Canada.}$

$$\text{i)} \quad \exists x \ M(x)$$

$$\text{ii)} \quad \forall x (C(x) \vee M(x))$$

Example: Express the statement "If somebody is female and is a parent, then this person is someone's mother" as a logical expression.

Example: Express the statement "If somebody is female and is a parent, then this person is someone's mother" as a logical expression.

Solution:

$$F(x) \equiv x \text{ is female}$$

$$P(x) \equiv x \text{ is a parent}$$

$$M(x,y) \equiv x \text{ is the mother of } y$$

$$\forall x (F(x) \wedge P(x)) \rightarrow \exists y M(x,y)$$

an equivalent expression: $\forall x \exists y ((F(x) \wedge p(x)) \rightarrow M(x,y))$

Example: Use quantifiers to express the statement -

"There is a woman who has taken a flight on every airline in the world"

Example: Use quantifiers to express the statement -

"There is a woman who has taken a flight on every airline in the world"

Solution:

$P(w, f) \equiv w \text{ has taken } f$

$Q(f, a) \equiv f \text{ is a flight on } a$

The universe of discourse for w , f and a consist of all the women in the world, all airplane flights, and all airlines.

Example: Use quantifiers to express the statement -

"There is a woman who has taken a flight on every airline in the world"

Solution:

$P(w, f) \equiv w \text{ has taken } f$

$Q(f, a) \equiv f \text{ is a flight on } a$

The universe of discourse for w , f and a consist of all the women in the world, all airplane flights, and all airlines.

$$\exists w \forall a \exists f (P(w, f) \wedge Q(f, a))$$

Example: "All Lions are fierce"

"Some Lions do not drink coffee"

"Some fierce creatures do not drink coffee"

Express these statements as a logical expression.
Universe of discourse is all creatures over the world.

Solution:

$P(x) \equiv x \text{ is a lion}$

$Q(x) \equiv x \text{ is fierce}$

$R(x) \equiv x \text{ drinks coffee}$

$\forall x (P(x) \rightarrow Q(x))$

$\exists x (P(x) \wedge \neg R(x))$

$\exists x (Q(x) \wedge \neg R(x))$

Universe of discourse is all creatures.

Example: Let $P(x,y)$ be the statement " $x+y=y+x$ ". What is the truth value of the quantification

$$\forall x \forall y P(x,y)$$

Example: Let $P(x,y)$ be the statement " $x+y=y+x$ ". What is the truth value of the quantification

$$\forall x \forall y P(x,y)$$

Solution: The quantification

$$\forall x \forall y P(x,y)$$

denotes the proposition

"For all real numbers x and for all real numbers y , it is true that $x+y=y+x$ ".

So the proposition

$$\forall x \forall y P(x,y)$$

is true.

Example: Let $Q(x,y)$ denote " $x+y=0$ ". What are the truth values of the quantifications

$$\exists y \forall x Q(x,y)$$

$$\forall x \exists y Q(x,y)$$

Example: Let $Q(x,y)$ denote " $x+y=0$ ". What are the truth values of the quantifications

$$\exists y \forall x Q(x,y)$$

Solution:

$\exists y \forall x Q(x,y)$ denotes the proposition

"There is a real number y such that for every real number x , $Q(x,y)$ is true".

No matter what value of y is chosen, there is only one value of x for which $x+y=0$. Since there is no real number y such that $x+y=0$ for all real numbers x . So $\exists y \forall x Q(x,y)$ is FALSE.

Example: Let $Q(x,y)$ denote " $x+y=0$ ". What are the truth values of the quantifications

$$\exists y \forall x Q(x,y)$$

$$\forall x \exists y Q(x,y)$$

$\forall x \exists y Q(x,y)$ denotes the proposition

"For every real number x there is a real number y such that $Q(x,y)$ is true."

Given a real number x , there is a real number y such that $x+y=0$; namely, $y=-x$. So $\forall x \exists y Q(x,y)$ is TRUE.

Quantification of Two Variables

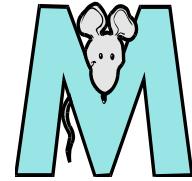
Statement	When True?	When False?
$\forall x \forall y P(x,y)$	$P(x,y)$ is true for every pair x,y .	There is a pair x,y for which $P(x,y)$ is false.
$\forall x \exists y P(x,y)$	For every x there is a y for which $P(x,y)$ is true.	There is an x such that $P(x,y)$ is false for every y .
$\exists x \forall y P(x,y)$	There is an x for which $P(x,y)$ is true for every y .	For every x there is a y for which $P(x,y)$ is false.
$\exists x \exists y P(x,y)$	There is a pair x,y for which $P(x,y)$ is true.	$P(x,y)$ is false for every pair x,y .
$\exists y \exists x P(x,y)$		

Negating Quantifiers

$$\neg \exists x P(x) \Leftrightarrow \forall x \neg P(x)$$

$$\neg \forall x P(x) \Leftrightarrow \exists x \neg P(x)$$

Example



Let $P(x)$ be the statement “the word x contains the letter m . ”

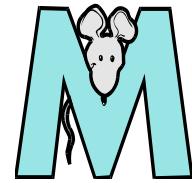
$$\neg \exists x P(x)$$

There is no word that contains the letter m .

$$\forall x \neg P(x)$$

For any word you pick, that word does not contain the letter m .

Example



Let $P(x)$ be the statement “the word x contains the letter m . ”

$$\neg \forall x P(x)$$

Not every word contains the letter m .

$$\exists x \neg P(x)$$

There is a word that does not contain the letter m .

We will often want to consider the negation of a quantified expression. For instance, consider the negation of the statement

"Every student in the class has taken a course in calculus"

This statement is a universal quantification, namely,

$$\forall x P(x)$$

where $P(x)$ is the statement "x has taken a course in calculus"

The negation of this statement is

"It is not the case that every student in the class has taken a course in calculus!"

Or this is equivalent to

"There is a student in the class who has not taken a course in calculus"

And this is simply the existential quantification of the negation of the original propositional function

$$\exists x \neg P(x)$$

This example illustrates the following equivalence:

$$\neg \forall x P(x) \Leftrightarrow \exists x \neg P(x).$$

Similarly the negation of $\exists x Q(x)$ is

$$\neg \exists x Q(x) \Leftrightarrow \forall x \neg Q(x)$$

Negation	Equivalent statement	When true?	When False?
$\neg \exists x P(x)$	$\forall x \neg P(x)$	$P(x)$ is false for every x .	There is an x for which $P(x)$ is true.
$\neg \forall x P(x)$	$\exists x \neg P(x)$	There is an x for which $P(x)$ is false.	$P(x)$ is true for every x .

Mat2033 - Discrete Mathematics

Methods of Proof

METHODS OF PROOF

The methods of proof discussed in this chapter are important not only because they are used to prove mathematical theorems, but also for their many applications to computer science. These applications include verifying that computer programs are correct, establishing that operating systems are secure, making inferences in the area of artificial intelligence, showing that system specifications are consistent, and so on. Consequently, understanding the techniques used in proofs is essential both in mathematics and in computer science.

Rules of Inference

We will now introduce rules of inference for propositional logic. These rules provide the justification of the steps used to show that a conclusion follows logically from a set of hypotheses. The tautology

$$(p \wedge (p \rightarrow q)) \rightarrow q$$

is the basis of the rule of inference called MODUS PONENS. This tautology is written in the following way

$$\begin{array}{c} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$$

Using this notation, the hypotheses are written in a column and the conclusion below a bar.

The symbol \therefore denotes "therefore." Modus ponens states that if both an implication and its hypotheses are known to be true, then the conclusion of this implication is true.

Example: Suppose that the implication

"If it snows today, then we will go skiing"

and its hypotheses,

"It is snowing today"

are true. Then, by modus ponens, it follows that the conclusion of the implication, "We will go skiing," is true.

Example: Assume that the implication

"If n is greater than 3, then n^2 is greater than 9"
is true. Consequently, if n is greater than 3, then, by
modus ponens, it follows that n^2 is greater than 9.

Table Lists some important rules of inference.

TABLE 1 Rules of Inference.

<i>Rule of Inference</i>	<i>Tautology</i>	<i>Name</i>
--------------------------	------------------	-------------

TABLE 1 Rules of Inference.

<i>Rule of Inference</i>	<i>Tautology</i>	<i>Name</i>
$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	Addition

TABLE 1 Rules of Inference.

<i>Rule of Inference</i>	<i>Tautology</i>	<i>Name</i>
$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Simplification

TABLE 1 Rules of Inference.

<i>Rule of Inference</i>	<i>Tautology</i>	<i>Name</i>
$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Simplification
$\frac{p \quad q}{\therefore p \wedge q}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction

TABLE 1 Rules of Inference.

<i>Rule of Inference</i>	<i>Tautology</i>	<i>Name</i>
$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Simplification
$\frac{p \qquad q}{\therefore p \wedge q}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\frac{p \qquad p \rightarrow q}{\therefore q}$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus ponens

TABLE 1 Rules of Inference.

<i>Rule of Inference</i>	<i>Tautology</i>	<i>Name</i>
$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Simplification
$\frac{p \qquad q}{\therefore p \wedge q}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\frac{p \qquad p \rightarrow q}{\therefore q}$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus ponens
$\frac{\neg q \qquad p \rightarrow q}{\therefore \neg p}$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus tollens

TABLE 1 Rules of Inference.

<i>Rule of Inference</i>	<i>Tautology</i>	<i>Name</i>
$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Simplification
$\frac{p \qquad q}{\therefore p \wedge q}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\frac{p \qquad p \rightarrow q}{\therefore q}$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus ponens
$\frac{\neg q \qquad p \rightarrow q}{\therefore \neg p}$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus tollens
$\frac{p \rightarrow q \qquad q \rightarrow r}{\therefore p \rightarrow r}$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Hypothetical syllogism

TABLE 1 Rules of Inference.

<i>Rule of Inference</i>	<i>Tautology</i>	<i>Name</i>
$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Simplification
$\frac{\begin{array}{c} p \\ q \end{array}}{\therefore p \wedge q}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\frac{\begin{array}{c} p \\ p \rightarrow q \end{array}}{\therefore q}$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus ponens
$\frac{\begin{array}{c} \neg q \\ p \rightarrow q \end{array}}{\therefore \neg p}$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus tollens
$\frac{\begin{array}{c} p \rightarrow q \\ q \rightarrow r \\ \therefore p \rightarrow r \end{array}}{}$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$\frac{p \vee q}{\therefore q}$	$[(p \vee q) \wedge \neg p] \rightarrow q$	Disjunctive syllogism

TABLE 1 Rules of Inference.

<i>Rule of Inference</i>	<i>Tautology</i>	<i>Name</i>
$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Simplification
$\frac{\begin{array}{c} p \\ q \end{array}}{\therefore p \wedge q}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\frac{\begin{array}{c} p \\ p \rightarrow q \end{array}}{\therefore q}$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus ponens
$\frac{\begin{array}{c} \neg q \\ p \rightarrow q \end{array}}{\therefore \neg p}$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus tollens
$\frac{\begin{array}{c} p \rightarrow q \\ q \rightarrow r \\ \therefore p \rightarrow r \end{array}}{}$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$\frac{\begin{array}{c} p \vee q \\ \neg p \end{array}}{\therefore q}$	$[(p \vee q) \wedge \neg p] \rightarrow q$	Disjunctive syllogism
$\frac{\begin{array}{c} p \vee q \\ \neg p \vee r \\ \therefore q \vee r \end{array}}{}$	$[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$	Resolution

Example: State which rule of inference is the basis of the following argument:

"It is below freezing now. Therefore, it is either below freezing or raining now."

Example: State which rule of inference is the basis of the following argument:

"It is below freezing now. Therefore, it is either below freezing or raining now."

Solution: Let p and q be:

p : It is below freezing now.

q : It is raining now.

Example: State which rule of inference is the basis of the following argument:

"It is below freezing now. Therefore, it is either below freezing or raining now."

Solution: Let p and q be:

p : It is below freezing now.

q : It is raining now.

Then this argument is of the form

$$\frac{P}{\therefore p \vee q}$$

Example: State which rule of inference is the basis of the following argument:

"It is below freezing now. Therefore, it is either below freezing or raining now."

Solution: Let p and q be:

p : It is below freezing now.

q : It is raining now.

Then this argument is of the form

$$\frac{p}{\therefore p \vee q}$$

This is an argument that uses the addition rule.

Example: State which rule of inference is the basis of the following argument "It is below freezing and raining now. Therefore, it is below freezing now."

Example: State which rule of inference is the basis of the following argument "It is below freezing and raining now. Therefore, it is below freezing now."

Solution: Let p and q be:

p : It is below freezing now

q : It is raining now.

Example: State which rule of inference is the basis of the following argument "It is below freezing and raining now. Therefore, it is below freezing now."

Solution: Let p and q be:

p : It is below freezing now

q : It is raining now.

This argument is of the form

$$\frac{p \wedge q}{\therefore p}$$

Example: State which rule of inference is the basis of the following argument "It is below freezing and raining now. Therefore, it is below freezing now."

Solution: Let p and q be:

p : It is below freezing now

q : It is raining now.

This argument is of the form

$$\frac{p \wedge q}{\therefore p} \quad (\text{simplification rule})$$

Example: State which rule of inference is used in the argument:

If it rains today, then will not have a barbecue today. If we do not have a barbecue today, then we will have a barbecue tomorrow. Therefore, if it rains today, then we will have a barbecue tomorrow.

Example: State which rule of inference is used in the argument:

If it rains today, then will not have a barbecue today. If we do not have a barbecue today, then we will have a barbecue tomorrow. Therefore, if it rains today, then we will have a barbecue tomorrow.

Solution: Let propositions p , q and r be:

p : It is raining today.

q : We will not have a barbecue today.

r : We will have a barbecue tomorrow.

Solution: Let propositions P , q and r be:

P : It is raining today.

q : We will not have a barbecue today.

r : We will have a barbecue tomorrow.

Then this argument is of the form

Solution: Let propositions P, q and r be:

p : It is raining today.

q : We will not have a barbecue today.

r : We will have a barbecue tomorrow.

Then this argument is of the form

$$\begin{array}{c} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$$

Solution: Let propositions P, q and r be:

P : It is raining today.

q : We will not have a barbecue today.

r : We will have a barbecue tomorrow.

Then this argument is of the form

$$\begin{array}{c} P \rightarrow q \\ q \rightarrow r \\ \hline \therefore P \rightarrow r \quad (\text{Hypothetical syllogism}) \end{array}$$

These examples show how arguments in English can be analyzed using rules of inference.

Example: Show that the hypotheses "It is not sunny this afternoon and it is colder than yesterday," "We will go swimming only if it is sunny," "If we do not go swimming, then we will take a canoe trip," and "If we take a canoe trip, then we will be home by sunset" lead to the conclusion "We will be home by sunset."

Solution: Let p, q, r, s , and t be:

p : It is sunny this afternoon

q : It is colder than yesterday

r : We will go swimming

s : We will take a canoe trip

t : We will be home by sunset

Solution: Let p, q, r, s , and t be:

p : It is sunny this afternoon

q : It is colder than yesterday

r : We will go swimming

s : We will take a canoe trip

t : We will be home by sunset

Then the hypotheses become $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$,
and $s \rightarrow t$.

Then the hypotheses become $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$,
and $s \rightarrow t$.

Then the hypotheses become $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$,
and $s \rightarrow t$.

<u>Step</u>	<u>Reason</u>
1. $\neg p \wedge q$	hypothesis

Then the hypotheses become $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$,
and $s \rightarrow t$.

<u>Step</u>	<u>Reason</u>
1. $\neg p \wedge q$	hypothesis
2. $\neg p$	Simplification using step 1

Then the hypotheses become $\neg p \wedge q$, $\Gamma \rightarrow p$, $\neg r \rightarrow s$,
and $s \rightarrow t$.

<u>Step</u>	<u>Reason</u>
1. $\neg p \wedge q$	hypothesis
2. $\neg p$	Simplification using step 1
3. $\Gamma \rightarrow p$	Hypotheses

Then the hypotheses become $\neg p \wedge q$, $\Gamma \rightarrow p$, $\neg r \rightarrow s$, and $s \rightarrow t$.

<u>Step</u>	<u>Reason</u>
1. $\neg p \wedge q$	hypothesis
2. $\neg p$	Simplification using step 1
3. $\Gamma \rightarrow p$	Hypotheses
4. $\neg r$	Modus tollens using steps 2 and 3

Then the hypotheses become $\neg p \wedge q$, $\Gamma \rightarrow p$, $\neg r \rightarrow s$, and $s \rightarrow t$.

<u>Step</u>	<u>Reason</u>
1. $\neg p \wedge q$	hypothesis
2. $\neg p$	Simplification using step 1
3. $\Gamma \rightarrow p$	Hypotheses
4. $\neg r$	Modus tollens using steps 2 and 3
5. $\neg r \rightarrow s$	Hypotheses

Then the hypotheses become $\neg p \wedge q$, $\Gamma \rightarrow p$, $\neg r \rightarrow s$, and $s \rightarrow t$.

<u>Step</u>	<u>Reason</u>
1. $\neg p \wedge q$	hypothesis
2. $\neg p$	Simplification using step 1
3. $\Gamma \rightarrow p$	Hypotheses
4. $\neg r$	Modus tollens using steps 2 and 3
5. $\neg r \rightarrow s$	Hypotheses
6. s	Modus ponens using steps 4 and 5

Then the hypotheses become $\neg p \wedge q$, $\Gamma \rightarrow p$, $\neg r \rightarrow s$, and $s \rightarrow t$.

<u>Step</u>	<u>Reason</u>
1. $\neg p \wedge q$	hypothesis
2. $\neg p$	Simplification using step 1
3. $\Gamma \rightarrow p$	Hypotheses
4. $\neg r$	Modus tollens using steps 2 and 3
5. $\neg r \rightarrow s$	Hypotheses
6. s	Modus ponens using steps 4 and 5
7. $s \rightarrow t$	Hypothesis

Then the hypotheses become $\neg p \wedge q$, $\Gamma \rightarrow p$, $\neg r \rightarrow s$, and $s \rightarrow t$.

<u>Step</u>	<u>Reason</u>
1. $\neg p \wedge q$	hypothesis
2. $\neg p$	Simplification using step 1
3. $\Gamma \rightarrow p$	Hypotheses
4. $\neg r$	Modus tollens using steps 2 and 3
5. $\neg r \rightarrow s$	Hypotheses
6. s	Modus ponens using steps 4 and 5
7. $s \rightarrow t$	Hypothesis
8. t	Modus ponens using steps 6 and 7

Example: Show that the hypotheses "If you send me an e-mail message, then I will finish writing the program," "If you do not send me an e-mail message, then I will go to sleep early," and "If I go to sleep early, then I will wake up feeling refreshed" lead to the conclusion "If I do not finish writing the program, then I will wake up feeling refreshed."

Example: Show that the hypotheses "If you send me an e-mail message, then I will finish writing the program," "If you do not send me an e-mail message, then I will go to sleep early," and "If I go to sleep early, then I will wake up feeling refreshed" lead to the conclusion "If I do not finish writing the program, then I will wake up feeling refreshed."

Solution: Let p, q, r, s, t be

p : You send me an e-mail message

q : I will finish writing the program

r : I will go to sleep early

s : I will wake up feeling refreshed

Example: Show that the hypotheses "If you send me an e-mail message, then I will finish writing the program," "If you do not send me an e-mail message, then I will go to sleep early," and "If I go to sleep early, then I will wake up feeling refreshed" lead to the conclusion "If I do not finish writing the program, then I will wake up feeling refreshed."

Solution: Let p, q, r, s, t be

p : You send me an e-mail message

q : I will finish writing the program

r : I will go to sleep early

s : I will wake up feeling refreshed

Then the hypotheses are $p \rightarrow q$, $\neg p \rightarrow r$, and $r \rightarrow s$.

p : You send me an e-mail message

q : I will finish writing the program

r : I will go to sleep early

s : I will wake up feeling refreshed

Then the hypotheses are $p \rightarrow q$, $\neg p \rightarrow r$, and $r \rightarrow s$.

p : You send me an e-mail message

q : I will finish writing the program

r : I will go to sleep early

s : I will wake up feeling refreshed

Then the hypotheses are $p \rightarrow q$, $\neg p \rightarrow r$, and $r \rightarrow s$.

<u>Step</u>	<u>Reason</u>
1. $p \rightarrow q$	Hypotheses

p : You send me an e-mail message

q : I will finish writing the program

r : I will go to sleep early

s : I will wake up feeling refreshed

Then the hypotheses are $p \rightarrow q$, $\neg p \rightarrow r$, and $r \rightarrow s$.

<u>Step</u>	<u>Reason</u>
1. $p \rightarrow q$	Hypotheses
2. $\neg q \rightarrow \neg p$	contrapositive of Step 1

p : You send me an e-mail message

q : I will finish writing the program

r : I will go to sleep early

s : I will wake up feeling refreshed

Then the hypotheses are $p \rightarrow q$, $\neg p \rightarrow r$, and $r \rightarrow s$.

<u>Step</u>	<u>Reason</u>
1. $p \rightarrow q$	Hypotheses
2. $\neg q \rightarrow \neg p$	contrapositive of Step 1
3. $\neg p \rightarrow r$	Hypotheses

p : You send me an e-mail message

q : I will finish writing the program

r : I will go to sleep early

s : I will wake up feeling refreshed

Then the hypotheses are $p \rightarrow q$, $\neg p \rightarrow r$, and $r \rightarrow s$.

<u>Step</u>	<u>Reason</u>
1. $p \rightarrow q$	Hypotheses
2. $\neg q \rightarrow \neg p$	contrapositive of Step 1
3. $\neg p \rightarrow r$	Hypotheses
4. $\neg q \rightarrow r$	Hypothetical syllogism using steps 2 and 3

p : You send me an e-mail message

q : I will finish writing the program

r : I will go to sleep early

s : I will wake up feeling refreshed

Then the hypotheses are $p \rightarrow q$, $\neg p \rightarrow r$, and $r \rightarrow s$.

<u>Step</u>	<u>Reason</u>
1. $p \rightarrow q$	Hypotheses
2. $\neg q \rightarrow \neg p$	contrapositive of Step 1
3. $\neg p \rightarrow r$	Hypotheses
4. $\neg q \rightarrow r$	Hypothetical syllogism using steps 2 and 3
5. $r \rightarrow s$	Hypotheses

p : You send me an e-mail message

q : I will finish writing the program

r : I will go to sleep early

s : I will wake up feeling refreshed

Then the hypotheses are $p \rightarrow q$, $\neg p \rightarrow r$, and $r \rightarrow s$.

<u>Step</u>	<u>Reason</u>
1. $p \rightarrow q$	Hypotheses
2. $\neg q \rightarrow \neg p$	contrapositive of Step 1
3. $\neg p \rightarrow r$	Hypotheses
4. $\neg q \rightarrow r$	Hypothetical syllogism using steps 2 and 3
5. $r \rightarrow s$	Hypotheses
6. $\neg q \rightarrow s$	Hypothetical syllogism using steps 4 and 5

Rules of Inference for Quantified Statements

We discussed rules of inference for propositions. We will now describe some important rules of inference for statements involving quantifiers.

Universal instantiation : is the rule of inference used to conclude that $P(c)$ is true, where c is a particular member of the universe of discourse, given the premise $\forall x P(x)$.

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Universal Generalization: is the rule of inference that states that $\forall x P(x)$ is true, given the premise that $P(c)$ is true for all elements c in the universe of discourse. Universal generalization is used when we show that $\forall x P(x)$ is true by taking an arbitrary element c from the universe of discourse and showing that $P(c)$ is true. The element c that we select must be an arbitrary, and not a specific element of the universe of discourse.

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

Existential instantiation : is the rule that allows us to conclude that there is an element c in the universe of discourse for which $P(c)$ is true if we know that $\exists x P(x)$ is true. We cannot select an arbitrary value of c here, but rather it must be a c for which $P(c)$ is true. Usually we have no knowledge of what c is, only that it exists. Since it exists, we may give it a name (c) and continue our argument.

$\exists x P(x)$

∴ $P(c)$ for some element c

Existential generalization : is the rule of inference that is used to conclude that $\exists x P(x)$ is true when a particular element c with $P(c)$ true is known. That is, if we know one element c in the universe of discourse for which $P(c)$ is true, then we know that $\exists x P(x)$ is true.

$P(c)$ for some element c

∴ $\exists x P(x)$

TABLE 2 Rules of Inference for Quantified Statements.

<i>Rule of Inference</i>	<i>Name</i>
$\frac{\forall x P(x)}{\therefore P(c)}$	Universal instantiation
$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$	Universal generalization
$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$	Existential instantiation
$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$	Existential generalization

EXAMPLE

Show that the premises “Everyone in this discrete mathematics class has taken a course in computer science” and “Marla is a student in this class” imply the conclusion “Marla has taken a course in computer science.”

EXAMPLE

Show that the premises “Everyone in this discrete mathematics class has taken a course in computer science” and “Marla is a student in this class” imply the conclusion “Marla has taken a course in computer science.”

Solution: Let $D(x)$ denote “ x is in this discrete mathematics class,” and let $C(x)$ denote “ x has taken a course in computer science.” Then the premises are $\forall x(D(x) \rightarrow C(x))$ and $D(\text{Marla})$. The conclusion is $C(\text{Marla})$.

EXAMPLE

Show that the premises “Everyone in this discrete mathematics class has taken a course in computer science” and “Marla is a student in this class” imply the conclusion “Marla has taken a course in computer science.”

Solution: Let $D(x)$ denote “ x is in this discrete mathematics class,” and let $C(x)$ denote “ x has taken a course in computer science.” Then the premises are $\forall x(D(x) \rightarrow C(x))$ and $D(\text{Marla})$. The conclusion is $C(\text{Marla})$.

The following steps can be used to establish the conclusion from the premises.

Step

1. $\forall x(D(x) \rightarrow C(x))$
2. $D(\text{Marla}) \rightarrow C(\text{Marla})$
3. $D(\text{Marla})$
4. $C(\text{Marla})$

Reason

- Premise
Universal instantiation from (1)
Premise
Modus ponens from (2) and (3)

EXAMPLE

Show that the premises “A student in this class has not read the book,” and “Everyone in this class passed the first exam” imply the conclusion “Someone who passed the first exam has not read the book.”

Solution: Let $C(x)$ be “ x is in this class,” $B(x)$ be “ x has read the book,” and $P(x)$ be “ x passed the first exam.” The premises are $\exists x(C(x) \wedge \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$. The conclusion is $\exists x(P(x) \wedge \neg B(x))$. These steps can be used to establish the conclusion from the premises.

Step

1. $\exists x(C(x) \wedge \neg B(x))$
2. $C(a) \wedge \neg B(a)$
3. $C(a)$
4. $\forall x(C(x) \rightarrow P(x))$
5. $C(a) \rightarrow P(a)$
6. $P(a)$
7. $\neg B(a)$
8. $P(a) \wedge \neg B(a)$
9. $\exists x(P(x) \wedge \neg B(x))$

Reason

- Premise
Existential instantiation from (1)
Simplification from (2)
Premise
Universal instantiation from (4)
Modus ponens from (3) and (5)
Simplification from (2)
Conjunction from (6) and (7)
Existential generalization from (8)

Methods of Proving Theorems

Direct Proofs

The implication $p \rightarrow q$ can be proved by showing that if p is true, then q must be true. This shows that the combination p true and q false never occurs. A proof of this kind is called a direct proof.

To carry out such a proof, assume that p is true and use rules of inference and theorems already proved to show that q must also be true.

Direct Proofs

- The implication $p \rightarrow q$ can be proved by showing that if p is true then q must also be true. This shows that the combination p true and q false never occurs.
- A proof of this kind is called a direct proof.

Example: Show that if $a|b$ and $b|c$ then $a|c$.

Proof: Assume that $a|b$ and $b|c$.

This means that there exists integer x and y such that $b = ax$ and $c = by$. But, by substitution we can then say that $c = (ax)y = a(xy)$. But xy is an integer, call it k . Therefore $c = ak$ and by the definition of divisibility, $a|c$.

Definition: The integer n is even if there exists an integer k such that $n=2k$ and it is odd if there exists an integer k such that $n=2k+1$.

Example: Give an indirect proof of the theorem "If n is odd, then n^2 is odd."

Solution: Assume that the hypotheses of the theorem is true, namely, suppose that n is odd. Then $n=2k+1$, where k is an integer. It follows that $n^2=(2k+1)^2=4k^2+4k+1=2(2k^2+2k)+1$. Therefore, n^2 is an odd integer.

Indirect Proofs

Since the implication $p \rightarrow q$ is equivalent to its contrapositive, $\neg q \rightarrow \neg p$, the implication $p \rightarrow q$ can be proved by showing that its contrapositive, $\neg q \rightarrow \neg p$, is true. This related implication is usually proved directly, but any proof technique can be used. An argument of this type is called an indirect proof.

Indirect Proof

- Since the implication $p \rightarrow q$ is equivalent to its contrapositive $\neg q \rightarrow \neg p$ the original implication can be proven by showing that the contrapositive is true.

Example: Show that if ab is even then a or b are even.

To prove a number is even you must show that it can be written as $2k$ for some integer k . Since we know that ab is even, $ab = 2k$ for some integer k . But what does that say about a and b ? Not much.

Consider the contrapositive of the implication:

If a and b are **not** even then ab is **not** even. That is, if a and b are odd then ab is odd.

Example – continued

If a number (ab in this case) is odd, we must show that it can be written as $2k+1$ for some integer k .

But, a and b are odd so there exists integers x and y such that $a=2x+1$ or $b=2y+1$.

Therefore,

$$ab = (2x+1)(2y+1) = 4xy + 2x + 2y + 1 = 2(2xy + x + y) + 1$$

Since $2xy+x+y$ is an integer (call it k) we can write ab as $2k+1$ and ab must be odd.

Example: Give an indirect proof of the theorem
"If $3n+2$ is odd, then n is odd."

Example: Give an indirect proof of the theorem
"If $3n+2$ is odd, then n is odd."

Solution: Assume that the conclusion of this implication
is false; namely assume that n is even. Then $n=2k$
for some integer k . It follows that $3n+2=3(2k)+2$
 $=6k+2=2(3k+1)$, so $3n+2$ is even and therefore
not odd. Because the negation of the conclusion of
the implication ~~implies~~ implies that the hypotheses
is false, the original implication is true.

Example: Prove that if n is an integer and n^2 is odd, then n is odd.

Example: Prove that if n is an integer and n^2 is odd, then n is odd.

Solution: Direct Proof: Suppose that n is an integer and n^2 is odd. Then, there exists an integer k such that $n^2 = 2k+1$. If we solve this equation for n we

get $n = \pm\sqrt{2k+1}$. But we can not say anything about n whether n is an odd or even integer. So direct proof does not give any result.

Indirect Proof: (We use $\neg q \rightarrow \neg p$, since this is equivalent $p \rightarrow q$.) Assume n is not odd. Then n is even and there exist an integer k such that $n = 2k$. By squaring both sides of this equation we get $n^2 = 4k^2 = 2(2k^2)$. Let $t = 2k^2$ then n^2 can be written as $n^2 = 2t$. This means n^2 is even. The proof is completed. This means that indirect proof gives the result.

Vacuous and Trivial Proofs

Suppose that the hypotheses p of an implication $p \rightarrow q$ is false. Then the implication is true, because the statement has the form $F \rightarrow T$ or $F \rightarrow F$, and hence is true. Consequently, if it can be shown that p is false, then a proof, called a vacuous proof, of the implication $p \rightarrow q$ can be given.

Exercise: Show that the proposition $P(0)$ is true where $P(n)$ is the propositional function "If $n > 1$, then $n^2 > n$."

Exercise: Show that the proposition $P(0)$ is true where $P(n)$ is the propositional function "If $n > 1$, then $n^2 > n$."

Solution: $P(0)$ is the implication "If $0 > 1$, then $0^2 > 0$." Since the hypothesis $0 > 1$ is false, the implication $P(0)$ is automatically true.

Trivial Proof

Suppose that the conclusion q of an implication $p \rightarrow q$ is true. Then $p \rightarrow q$ is true, since the statement has the form $T \rightarrow T$ or $F \rightarrow T$, which are true. Hence, if it can be shown that q is true, then a proof, called a trivial proof, of $p \rightarrow q$ can be given.

EXAMPLE

Let $P(n)$ be “If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$,” where the domain consists of all integers. Show that $P(0)$ is true.

EXAMPLE

Let $P(n)$ be “If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$,” where the domain consists of all integers. Show that $P(0)$ is true.

Solution: The proposition $P(0)$ is “If $a \geq b$, then $a^0 \geq b^0$.” Because $a^0 = b^0 = 1$, the conclusion of the conditional statement “If $a \geq b$, then $a^0 \geq b^0$ ” is true. Hence, this conditional statement, which is $P(0)$, is true. This is an example of a trivial proof. Note that the hypothesis, which is the statement “ $a \geq b$,” was not needed in this proof. ◀

Example: Prove that the sum of two rational numbers is rational.

Solution: (The real number r is rational if there exist integers p and q with $q \neq 0$ such that $r = \frac{p}{q}$. A real number that is not rational is called irrational)

Direct Proof: Let $r, s \in \mathbb{Q}$. Then there exists integers p, q, t, u such that $r = \frac{p}{q}$ ($q \neq 0$) and $s = \frac{t}{u}$ ($u \neq 0$)

$$r+s = \frac{p}{q} + \frac{t}{u} = \frac{pu+ tq}{uq} \quad (\text{since } u \neq 0, q \neq 0)$$

Therefore $r+s$ is rational.

Vacuous Proof Example

Theorem. (For all n) If n is both odd and even, then $n^2 = n + n$.

Proof. The statement “ n is both odd and even” is necessarily false, since no number can be both odd and even. So, the theorem is vacuously true.

□

Trivial Proof Example

Theorem. (For integers n) If n is the sum of two prime numbers, then either n is odd or n is even.

Proof. Any integer n is either odd or even. So the conclusion of the implication is true regardless of the truth of the antecedent. Thus the implication is true trivially. \square

Mat2033 - Discrete Mathematics

Methods of Proving Theorems

Methods of Proving Theorems

Direct Proofs

The implication $p \rightarrow q$ can be proved by showing that if p is true, then q must be true. This shows that the combination p true and q false never occurs. A proof of this kind is called a direct proof.

To carry out such a proof, assume that p is true and use rules of inference and theorems already proved to show that q must also be true.

Direct Proofs

- The implication $p \rightarrow q$ can be proved by showing that if p is true then q must also be true. This shows that the combination p true and q false never occurs.
- A proof of this kind is called a direct proof.

Example: Show that if $a|b$ and $b|c$ then $a|c$.

Proof: Assume that $a|b$ and $b|c$.

This means that there exists integer x and y such that $b = ax$ and $c = by$. But, by substitution we can then say that $c = (ax)y = a(xy)$. But xy is an integer, call it k . Therefore $c = ak$ and by the definition of divisibility, $a|c$.

Definition: The integer n is even if there exists an integer k such that $n=2k$ and it is odd if there exists an integer k such that $n=2k+1$.

Example: Give an indirect proof of the theorem "If n is odd, then n^2 is odd."

Solution: Assume that the hypotheses of the theorem is true, namely, suppose that n is odd. Then $n=2k+1$, where k is an integer. It follows that $n^2=(2k+1)^2=4k^2+4k+1=2(2k^2+2k)+1$. Therefore, n^2 is an odd integer.

Indirect Proofs

Since the implication $p \rightarrow q$ is equivalent to its contrapositive, $\neg q \rightarrow \neg p$, the implication $p \rightarrow q$ can be proved by showing that its contrapositive, $\neg q \rightarrow \neg p$, is true. This related implication is usually proved directly, but any proof technique can be used. An argument of this type is called an indirect proof.

Indirect Proof

- Since the implication $p \rightarrow q$ is equivalent to its contrapositive $\neg q \rightarrow \neg p$ the original implication can be proven by showing that the contrapositive is true.

Example: Show that if ab is even then a or b are even.

To prove a number is even you must show that it can be written as $2k$ for some integer k . Since we know that ab is even, $ab = 2k$ for some integer k . But what does that say about a and b ? Not much.

Consider the contrapositive of the implication:

If a and b are **not** even then ab is **not** even. That is, if a and b are odd then ab is odd.

Example – continued

If a number (ab in this case) is odd, we must show that it can be written as $2k+1$ for some integer k .

But, a and b are odd so there exists integers x and y such that $a=2x+1$ or $b=2y+1$.

Therefore,

$$ab = (2x+1)(2y+1) = 4xy + 2x + 2y + 1 = 2(2xy + x + y) + 1$$

Since $2xy+x+y$ is an integer (call it k) we can write ab as $2k+1$ and ab must be odd.

Example: Give an indirect proof of the theorem
"If $3n+2$ is odd, then n is odd."

Example: Give an indirect proof of the theorem
"If $3n+2$ is odd, then n is odd."

Solution: Assume that the conclusion of this implication
is false; namely assume that n is even. Then $n=2k$
for some integer k . It follows that $3n+2=3(2k)+2$
 $=6k+2=2(3k+1)$, so $3n+2$ is even and therefore
not odd. Because the negation of the conclusion of
the implication ~~implies~~ implies that the hypotheses
is false, the original implication is true.

Example: Prove that if n is an integer and n^2 is odd, then n is odd.

Example: Prove that if n is an integer and n^2 is odd, then n is odd.

Solution: Direct Proof: Suppose that n is an integer and n^2 is odd. Then, there exists an integer k such that $n^2 = 2k+1$. If we solve this equation for n we

get $n = \pm\sqrt{2k+1}$. But we can not say anything about n whether n is an odd or even integer. So direct proof does not give any result.

Indirect Proof: (We use $\neg q \rightarrow \neg p$, since this is equivalent $p \rightarrow q$.) Assume n is not odd. Then n is even and there exist an integer k such that $n = 2k$. By squaring both sides of this equation we get $n^2 = 4k^2 = 2(2k^2)$. Let $t = 2k^2$ then n^2 can be written as $n^2 = 2t$. This means n^2 is even. The proof is completed. This means that indirect proof gives the result.

Vacuous and Trivial Proofs

Suppose that the hypotheses p of an implication $p \rightarrow q$ is false. Then the implication is true, because the statement has the form $F \rightarrow T$ or $F \rightarrow F$, and hence is true. Consequently, if it can be shown that p is false, then a proof, called a vacuous proof, of the implication $p \rightarrow q$ can be given.

Exercise: Show that the proposition $P(0)$ is true where $P(n)$ is the propositional function "If $n > 1$, then $n^2 > n$."

Exercise: Show that the proposition $P(0)$ is true where $P(n)$ is the propositional function "If $n > 1$, then $n^2 > n$."

Solution: $P(0)$ is the implication "If $0 > 1$, then $0^2 > 0$." Since the hypothesis $0 > 1$ is false, the implication $P(0)$ is automatically true.

Trivial Proof

Suppose that the conclusion q of an implication $p \rightarrow q$ is true. Then $p \rightarrow q$ is true, since the statement has the form $T \rightarrow T$ or $F \rightarrow T$, which are true. Hence, if it can be shown that q is true, then a proof, called a trivial proof, of $p \rightarrow q$ can be given.

EXAMPLE

Let $P(n)$ be “If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$,” where the domain consists of all integers. Show that $P(0)$ is true.

EXAMPLE

Let $P(n)$ be “If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$,” where the domain consists of all integers. Show that $P(0)$ is true.

Solution: The proposition $P(0)$ is “If $a \geq b$, then $a^0 \geq b^0$.” Because $a^0 = b^0 = 1$, the conclusion of the conditional statement “If $a \geq b$, then $a^0 \geq b^0$ ” is true. Hence, this conditional statement, which is $P(0)$, is true. This is an example of a trivial proof. Note that the hypothesis, which is the statement “ $a \geq b$,” was not needed in this proof. ◀

Example: Prove that the sum of two rational numbers is rational.

Solution: (The real number r is rational if there exist integers p and q with $q \neq 0$ such that $r = \frac{p}{q}$. A real number that is not rational is called irrational)

Direct Proof: Let $r, s \in \mathbb{Q}$. Then there exists integers p, q, t, u such that $r = \frac{p}{q}$ ($q \neq 0$) and $s = \frac{t}{u}$ ($u \neq 0$)

$$r+s = \frac{p}{q} + \frac{t}{u} = \frac{pu+ tq}{uq} \quad (uq \neq 0 \text{ since } u \neq 0, q \neq 0)$$

Therefore $r+s$ is rational.

Vacuous Proof Example

Theorem. (For all n) If n is both odd and even, then $n^2 = n + n$.

Proof. The statement “ n is both odd and even” is necessarily false, since no number can be both odd and even. So, the theorem is vacuously true.

□

Trivial Proof Example

Theorem. (For integers n) If n is the sum of two prime numbers, then either n is odd or n is even.

Proof. Any integer n is either odd or even. So the conclusion of the implication is true regardless of the truth of the antecedent. Thus the implication is true trivially. \square

Proof by Contradiction

- We want to prove that a statement p is true.
- Suppose that a contradiction q can be found so that $\neg p \rightarrow q$ is true, that is, $\neg p \rightarrow F$ true. Then the proposition $\neg p$ must be false and consequently p must be true.
- This technique can be used when a contradiction, such as $r \wedge \neg r$, can be found so that it is possible to show that the implication $\neg p \rightarrow (r \wedge \neg r)$ is true.
- An argument of this type is called a proof by contradiction.

Example: Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

Solution: Let p be the proposition " $\sqrt{2}$ is irrational". Suppose that $\neg p$ is true. Then $\sqrt{2}$ is rational. We will show that this leads to a contradiction. Under the assumption that that $\sqrt{2}$ is rational, there exist integers a and b with $\sqrt{2} = \frac{a}{b}$, where a and b have no common factors (so that the fraction $\frac{a}{b}$ is in lowest terms). Since $\sqrt{2} = \frac{a}{b}$, when both sides of this equation are squared, it follows that

$$2 = \frac{a^2}{b^2}$$

Hence,

$$2b^2 = a^2.$$

This means that a^2 is even, implying that a is even.

Furthermore, since a is even, $a=2c$ for some integer c .

Thus

$$2b^2 = 4c^2$$

so

$$b^2 = 2c^2$$

This means that b^2 is even. Hence, b must be even as well.

It has been shown that $\neg p$ implies that $\sqrt{2} = \frac{a}{b}$, where a and b have no common factors, and 2 divides a and b . This is a contradiction since we have shown that $\neg p$ implies both Γ and $\neg\Gamma$ where Γ is the statement that a and b are integers with no common factors. Hence, $\neg p$ is false, so that p : " $\sqrt{2}$ is irrational" is true.

Existence Proofs

Many theorems are assertions that objects of a particular type exist. A theorem of this type is a proposition of the form $\exists x P(x)$, where P is a predicate. A proof of a proposition of the form $\exists x P(x)$ is called an existence proof. There are several ways to prove a theorem of this type. Sometimes an existence proof of $\exists x P(x)$ can be given by finding an element a such that $P(a)$ is true.

Such an existence proof is called constructive. It is also possible to give an existence proof that is nonconstructive; that is, we do not find an element a such that $P(a)$ is true, but rather prove that $\exists x P(x)$ is true in some other way. One common method of giving a nonconstructive existence proof is to use proof by contradiction and show that the negation of the existential quantification implies a contradiction.

Example: (A constructive Existence Proof): Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Solution: After considerable computation we find that

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

We have proved the assertion.

Example: (A nonconstructive Existence Proof): Show that there exist irrational numbers x and y such that x^y is rational.

Example: (A nonconstructive Existence Proof): Show that there exist irrational numbers x and y such that x^y is rational.

Solution: $\sqrt{2}$ is irrational. Let $x = \sqrt{2}$ and $y = \sqrt{2}$. Consider the number $\sqrt{2}^{\sqrt{2}}$. If it is rational, we have two irrational numbers x and y with x^y rational. On the other hand if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ so that $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\sqrt{2}} = (\sqrt{2})^2 = 2$. We have shown that either the pair $x = \sqrt{2}$, $y = \sqrt{2}$ or the pair $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$ have the desired property, but we do not know which of these two pairs work!

Nonconstructive Existence Proof

Theorem: There are infinitely many prime numbers.

- Any finite set of numbers must contain a maximal element, so we can prove the theorem if we can just show that there is *no* largest prime number.
- *I.e.*, show that for any prime number, there is a larger number that is *also* prime.
- More generally: For any number, \exists a larger prime.
- Formally: Show $\forall n \exists p > n : p \text{ is prime}$.

- Given $n > 0$, prove there is a prime $p > n$.
- Consider $x = n! + 1$. Since $x > 1$, we know $(x \text{ is prime}) \vee (x \text{ is composite})$.
- **Case 1:** x is prime. Obviously $x > n$, so let $p = x$ and we're done.
- **Case 2:** x has a prime factor p . But if $p \leq n$, then p divides 1. So $p > n$, and we're done.

Uniqueness Proofs

Some theorems assert the existence of a unique element with a particular property. In other words, these theorems assert that there is exactly one element with this property. To prove a statement of this type we need to show that an element with this property exists and that no other element has this property. The two parts of a uniqueness proof are:

Existence: We show that an element x with the desired property exists.

Uniqueness: We show that if $y \neq x$, then y does not have the desired property.

Remark: Showing that there is a unique element x such that $P(x)$ is the same as proving the statement

$$\exists x (P(x) \wedge \forall y (y \neq x \rightarrow \neg P(y))).$$

~~E~~ Example: Show that every integer has a unique additive inverse. Show that if p is an integer, then there exists a unique integer q such that $p+q=0$.

Example: Show that every integer has a unique additive inverse. Show that if p is an integer, then there exists a unique integer q such that $p+q=0$.

Solution: If p is an integer, we find that $p+q=0$ when $q=-p$ and q is also an integer. To show that q is unique suppose r is an integer with $r \neq q$ such that $p+r=0$. Then

$$\begin{aligned} p+q &= p+r \\ p-p &= r-q = 0 \Rightarrow r=q. \end{aligned}$$

We find $r=q$ which contradicts our assumption. Consequently there exist a unique integer q such that $p+q=0$.

EXAMPLE

Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Solution: First, note that the real number $r = -b/a$ is a solution of $ar + b = 0$ because $a(-b/a) + b = -b + b = 0$. Consequently, a real number r exists for which $ar + b = 0$. This is the existence part of the proof.

Second, suppose that s is a real number such that $as + b = 0$. Then $ar + b = as + b$, where $r = -b/a$. Subtracting b from both sides, we find that $ar = as$. Dividing both sides of this last equation by a , which is nonzero, we see that $r = s$. This means that if $s \neq r$, then $as + b \neq 0$. This establishes the uniqueness part of the proof. ◀

Counterexamples

We can show that a statement of the form $\forall x P(x)$ is false if we can find a counterexample, that is, an example x for which $P(x)$ is false.

Example: "Every positive integer is the sum of the squares of three integers". Show that this is false.

Solution: If we can show that there is a particular integer that is not the sum of the squares of three integers then the statement is false. To look for a counterexample, we try to write successive positive integers as a sum of three squares. We find that

$$1 = \rho^2 + \rho^2 + 1^2$$

$$1 = \rho^2 + \rho^2 + t^2$$

$$\rho \approx \rho^2 + t^2 + t^2$$

$$1 = \rho^2 + \rho^2 + 1^2$$

$$2 \leq \rho^2 + 1^2 + 1^2$$

$$3 \leq 1^2 + 1^2 + 1^2$$

$$1 = 0^2 + 0^2 + 1^2$$

$$2 = 0^2 + 1^2 + 1^2$$

$$3 = 1^2 + 1^2 + 1^2$$

$$4 = 0^2 + 0^2 + 2^2$$

$$1 = 0^2 + 0^2 + 1^2$$

$$2 = 0^2 + 1^2 + 1^2$$

$$3 = 1^2 + 1^2 + 1^2$$

$$4 = 0^2 + 0^2 + \underline{2}^2$$

$$5 = 0^2 + 1^2 + \underline{2}^2$$

$$1 = 0^2 + 0^2 + 1^2$$

$$2 = 0^2 + 1^2 + 1^2$$

$$3 = 1^2 + 1^2 + 1^2$$

$$4 = 0^2 + 0^2 + 2^2$$

$$5 = 0^2 + 1^2 + 2^2$$

$$6 = 1^2 + 1^2 + 2^2$$

$$1 = 0^2 + 0^2 + 1^2$$

$$2 = 0^2 + 1^2 + 1^2$$

$$3 = 1^2 + 1^2 + 1^2$$

$$4 = 0^2 + 0^2 + 2^2$$

$$5 = 0^2 + 1^2 + 2^2$$

$$6 = 1^2 + 1^2 + 2^2$$

But we can not write 7 as the sum of three squares. 7 is a counterexample. We conclude that the statement is false.

Mathematical induction

- Frequently we want to prove a proposition of the form $\forall n P(n)$, in which the universe of discourse is the set of positive integers.

Mathematical induction

- Principle of Mathematical Induction (weak induction): Suppose that $P(1)$ is true and that for every positive integer n , if $P(n)$ is true then $P(n+1)$ is true as well. Then for every positive integer n , the proposition $P(n)$ is true.
- Principle of Mathematical Induction (strong induction): Suppose that $P(1)$ is true and that for every positive integer n , if $P(1), P(2), \dots, P(n)$ are true then $P(n+1)$ is true as well. Then for every positive integer n , the proposition $P(n)$ is true.

Well-Ordering Principle: Every nonempty set of positive integers has a least element.

Mathematical induction

- Intuitively the idea of induction is this. I prove $P(1)$. This is called the ***basis step***. Then for a fixed but arbitrary n , I assume $P(n)$ is true and I use it to prove $P(n+1)$. This is called the ***inductive step***, and the assumption that $P(n)$ is true is called the ***induction hypothesis*** (sometimes IH for short). Thus $P(n) \rightarrow P(n+1)$ is always true. Since, $P(1)$ is true, then $P(2)$ is as well. So $P(3)$ is, and thus $P(4)$ is, etc. It is typical to require beginning students to label their basis and inductive steps. With practice, however, mathematicians find that induction proofs are usually mechanical, and they write them quite casually.

Mathematical induction

Example: The sum of the first n positive odd integers is n^2 . That is, for all positive integers,

$$1 + 3 + \dots + (2n-1) = n^2.$$

Solution:

1. Basis Step: If $n=1$, the proposition states that

$$1 = 1^2,$$

which is true.

2. Induction Hypothesis: For some positive integer n , assume the proposition holds. That is, assume

$$1 + 3 + \dots + (2n-1) = n^2.$$

Mathematical induction

Example: The sum of the first n positive odd integers is n^2 . That is, for all positive integers,

$$1 + 3 + \dots + (2n-1) = n^2.$$

Solution:

3. Inductive Step: We want to show that it also holds for $n+1$.

That is, we want to show

$$1 + 3 + \dots + (2n-1) + (2n+1) = (n+1)^2.$$

Using the induction hypothesis we see

$$[1+3+\dots+(2n-1)] + (2n+1) = n^2 + (2n+1) = (n+1)^2.$$

By the principle of mathematical induction,

$$1 + 3 + \dots + (2n-1) = n^2$$

for all positive integers n .

Example: If n is a positive integer, then $n^3 - n$ is a multiple of 3.

Solution:

1. Basis Step: If $n=1$, then we have

$$1^3 - 1 = 0 = 3 \cdot 0,$$

which is a multiple of 3.

2. Induction Hypothesis: For some positive integer n , assume $n^3 - n$ is a multiple of 3. So, for instance, $n^3 - n = 3m$, for some integer m .

Example: If n is a positive integer, then $n^3 - n$ is a multiple of 3.

Solution:

3. Inductive Step: We wish to show

$$(n+1)^3 - (n+1) \text{ is a multiple of 3.}$$

We may rewrite

$$\begin{aligned}(n+1)^3 - (n+1) &= (n^3 + 3n^2 + 3n + 1) - (n+1) \\&= (n^3 - n) + 3n^2 + 3n \\&= 3m + 3n^2 + 3n \\&= 3(m+n^2+n),\end{aligned}$$

which is a multiple of 3.

Therefore by the principle of mathematical induction, for all positive integers n , it holds that $n^3 - n$ is a multiple of 3.

Theorem: Every positive integer greater than 1 has a prime factor.

Proof:

1. Basis Step: The positive integer 2 has itself for a prime factor.

2. Induction Hypothesis: For some positive integer n , suppose integers 2, 3, 4, ..., n all have prime factors.

3. Inductive Step: We want to show that $n+1$ has a prime factor. Let us consider two cases: If $n+1$ is prime, then it is a prime factor of itself. If $n+1$ is not prime, it has factors a and b such that $n+1=ab$. Necessarily a and b are smaller than $n+1$. Therefore by the induction hypothesis a has a prime factor, say p . Then $n+1=ab$. But p is a factor of a and therefore of ab , so $n+1$ has a prime factor. By the principle of mathematical induction, every positive integers greater than 1 has a prime factor.

Mat2033 - Discrete Mathematics

Set Theory

Introduction to Set Theory

- A set is a new type of structure, representing an **unordered** collection (group, plurality) of zero or more **distinct** (different) objects.
- Set theory deals with operations between, relations among, and statements about sets.
- All of mathematics can be defined in terms of some form of set theory (using predicate logic).

Basic notations for sets

- For sets, we'll use variables S, T, U, \dots
- We can denote a set S in writing by listing all of its elements in curly braces:
 - $\{a, b, c\}$ is the set of whatever 3 objects are denoted by a, b, c .
- Set builder notation: For any proposition $P(x)$ over any universe of discourse, $\{x | P(x)\}$ is the set of all x such that $P(x)$.

Basic properties of sets

- Sets are inherently unordered:
 - No matter what objects a , b , and c denote,
 $\{a, b, c\} = \{a, c, b\} = \{b, a, c\} =$
 $\{b, c, a\} = \{c, a, b\} = \{c, b, a\}.$
- All elements are distinct (unequal); multiple listings make no difference!
 - If $a=b$, then
 $\{a,b,c\}=\{a,c\}=\{b,c\}=\{a,a,b,a,b,c,c,c,c\}.$
 - This set contains at most 2 elements!

Definition of Set Equality

- Two sets are declared to be equal if and only if they contain *exactly the same elements*.
- In particular, it does not matter how the set is defined or denoted.
- For example: The set

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

$=\{x \mid x \text{ is an integer where } 0 < x < 5\}$

$=\{x \mid x \text{ is a positive integer where } 0 < x^2 < 25\}$

Infinite Sets

- Conceptually, sets may be infinite
- Symbols for some special infinite sets:

$\mathbb{N} = \{0, 1, 2, \dots\}$ The Natural numbers.

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ The Integers.

\mathbb{R} = The Real numbers.

Basic Set Relations: Member of

- $x \in S$ (“ x is in S ”) is the proposition that object x is an element or member of set S .
 - e.g. $3 \in \mathbb{N}$,
 - “ a ” $\in \{x \mid x \text{ is a letter of the alphabet}\}$
 - Can define set equality in terms of \in relation:
$$\forall S, T: S = T \leftrightarrow (\forall x: x \in S \leftrightarrow x \in T)$$
“Two sets are equal iff they have all the same members.”
- $x \notin S := \neg(x \in S)$ “ x is not in S ”

The Empty Set

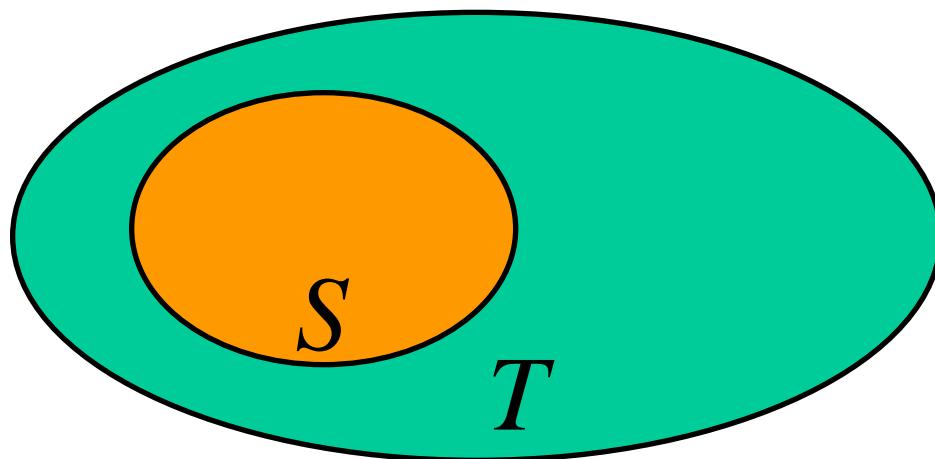
- \emptyset (“null set”, “empty set”) is the unique set that contains no elements whatsoever.
- $\emptyset = \{\}$
- No matter what is the domain of discourse (or u.d.), we have the axiom
 $\neg\exists x: x \in \emptyset$.

Subset and Superset Relations

- $S \subseteq T$ (“S is a subset of T”) means that every element of S is also an element of T.
- $S \subseteq T \Leftrightarrow \forall x (x \in S \rightarrow x \in T)$
- $\emptyset \subseteq S$, $S \subseteq S$.
- $S \supseteq T$ (“S is a superset of T”) means $T \subseteq S$.
- Note $S = T \Leftrightarrow S \subseteq T \wedge S \supseteq T$.
- $S \not\subseteq T$ means $\neg(S \subseteq T)$, i.e. $\exists x(x \in S \wedge x \notin T)$

Proper (Strict) Subsets & Supersets

- $S \subset T$ (“S is a proper subset of T”) means that $S \subseteq T$ but $T \not\subseteq S$. Similar for $S \supset T$.



Example:
 $\{1,2\} \subset \{1,2,3\}$

Venn Diagram equivalent of $S \subset T$

Sets Are Objects, Too!

- The objects that are elements of a set may themselves be sets.
- E.g. let $S=\{x \mid x \subseteq \{1,2,3\}\}$, then
 $S=\{\emptyset, \{1\}, \{2\}, \{3\},$
 $\{1,2\}, \{1,3\}, \{2,3\},$
 $\{1,2,3\}\}$
- Note that $1 \neq \{1\} \neq \{\{1\}\}$!!!!

Cardinality and Finiteness

- $|S|$ (read “the cardinality of S ”) is a measure of how many different elements S has.
- E.g., $|\emptyset|=0$, $|\{1,2,3\}| = 3$, $|\{a,b\}| = 2$,
 $|\{\{1,2,3\},\{4,5\}\}| = \underline{\underline{2}}$
- If $|S| \in \mathbb{N}$, then we say S is finite.
Otherwise, we say S is infinite.
- What are some infinite sets we’ve seen?
 $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \dots$

The Power Set Operation

- The power set $P(S)$ of a set S is the set of all subsets of S . $P(S) = \{x \mid x \subseteq S\}$.
- E.g. $P(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$.
- Sometimes $P(S)$ is written 2^S . Note that for finite S , $|P(S)| = 2^{|S|}$.
- It turns out that $|P(N)| > |N|$. There are different sizes of infinite sets!

Review: Set Notations So Far

- Variable objects x, y, z ; sets S, T, U .
- Literal set $\{a, b, c\}$ and set–builder $\{x \mid P(x)\}$.
- \in relational operator, and the empty set \emptyset .
- Set relations $=, \subseteq, \supseteq, \subset, \supset, \not\subset$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Power sets $P(S)$.

Ordered n-tuples

- These are like sets, except that duplicates matter, and the order makes a difference.
- For $n \in \mathbb{N}$, an ordered n-tuple or a sequence of length n is written (a_1, a_2, \dots, a_n) . The first element is a_1 , the second element is a_2 , etc.
- Note $(1, 2) \neq (2, 1) \neq (2, 1, 1)$.
- Empty sequence, singlets, pairs, triples, quadruples, quintuples, ..., n-tuples.

Cartesian Products of Sets

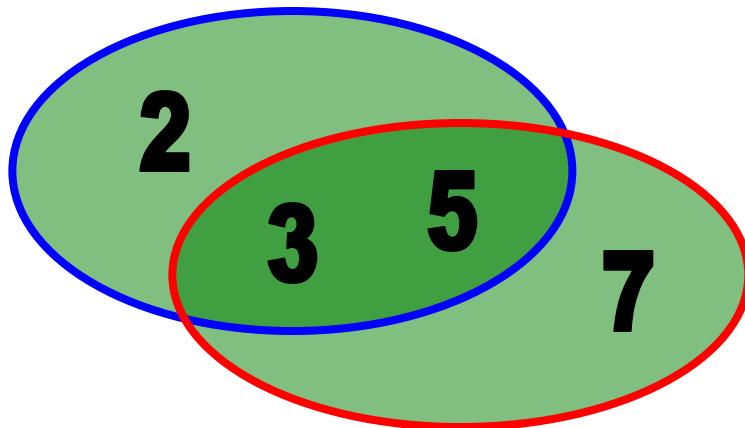
- For sets A, B, their Cartesian product
$$A \times B := \{(a, b) \mid a \in A \wedge b \in B\}.$$
- E.g. $\{a,b\} \times \{1,2\} = \{(a,1), (a,2), (b,1), (b,2)\}$
- Note that for finite A, B,
$$|A \times B| = |A| \cdot |B|$$
- Note that the Cartesian product is not commutative: $\neg \forall A, B: A \times B = B \times A$.
- Extends to $A_1 \times A_2 \times \dots \times A_n \dots$

The Union Operator

- For sets A , B , their union $A \cup B$ is the set containing all elements that are either in A , or (“ \vee ”) in B (or, of course, in both).
- Formally, $\forall A, B: A \cup B = \{x \mid x \in A \vee x \in B\}$.
- Note that $A \cup B$ contains all the elements of A **and** it contains all the elements of B :
$$\forall A, B: ((A \cup B) \supseteq A) \wedge ((A \cup B) \supseteq B)$$

Union Examples

- $\{a,b,c\} \cup \{2,3\} = \{a,b,c,2,3\}$
- $\{2,3,5\} \cup \{3,5,7\} = \{2,3,5,3,5,7\}$
 $= \{2,3,5,7\}$



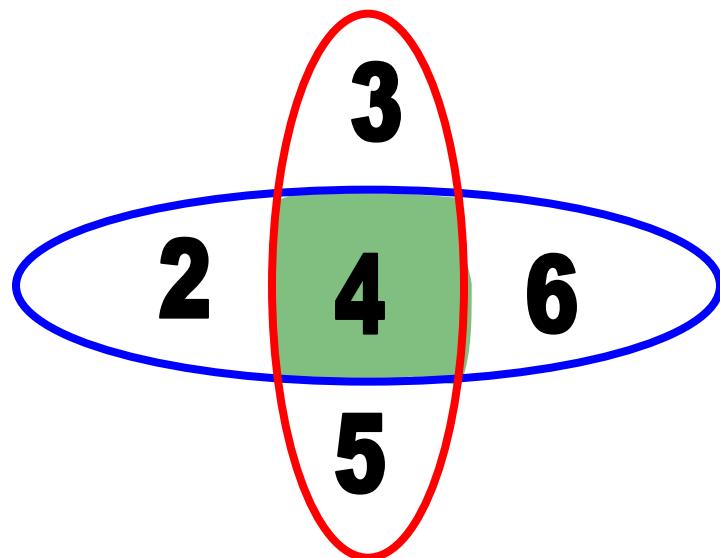
The Intersection Operator

- For sets A , B , their intersection $A \cap B$ is the set containing all elements that are simultaneously in A **and** (“ \wedge ”) in B .
- Formally, $\forall A, B: A \cap B \equiv \{x \mid x \in A \wedge x \in B\}$.
- Note that $A \cap B$ is a subset of A **and** it is a subset of B :

$$\forall A, B: ((A \cap B) \subseteq A) \wedge ((A \cap B) \subseteq B)$$

Intersection Examples

- $\{a,b,c\} \cap \{2,3\} = \underline{\emptyset}$
- $\{2,4,6\} \cap \{3,4,5\} = \underline{\{4\}}$



Disjointedness

- Two sets A , B are called disjoint (i.e., unjoined) iff their intersection is empty. ($A \cap B = \emptyset$)
- Example: the set of even integers is disjoint with the set of odd integers.

Inclusion–Exclusion Principle

- How many elements are in $A \cup B$?

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Example:

How many positive integers between 50 and 100

- a) are divisible by 7? Which integers are these?
- b) are divisible by 11? Which integers are these?
- c) are divisible by both 7 and 11? Which integers are these?
- d) are divisible by 7 or 11? Which integers are these?

a) Seven: 56, 63, 70, 77, 84, 91, 98

b) Five: 55, 66, 77, 88, 99

c) One: 77

d) Eleven: 55, 56, 63, 66, 70, 77, 84, 88, 91, 98, 99

Set Difference

- For sets A , B , the difference of A and B , written $A - B$, is the set of all elements that are in A but not B .
- $$\begin{aligned} A - B &= \{x \mid x \in A \wedge x \notin B\} \\ &= \{x \mid \neg(x \in A \rightarrow x \in B)\} \end{aligned}$$
- Also called:
The complement of B with respect to A .

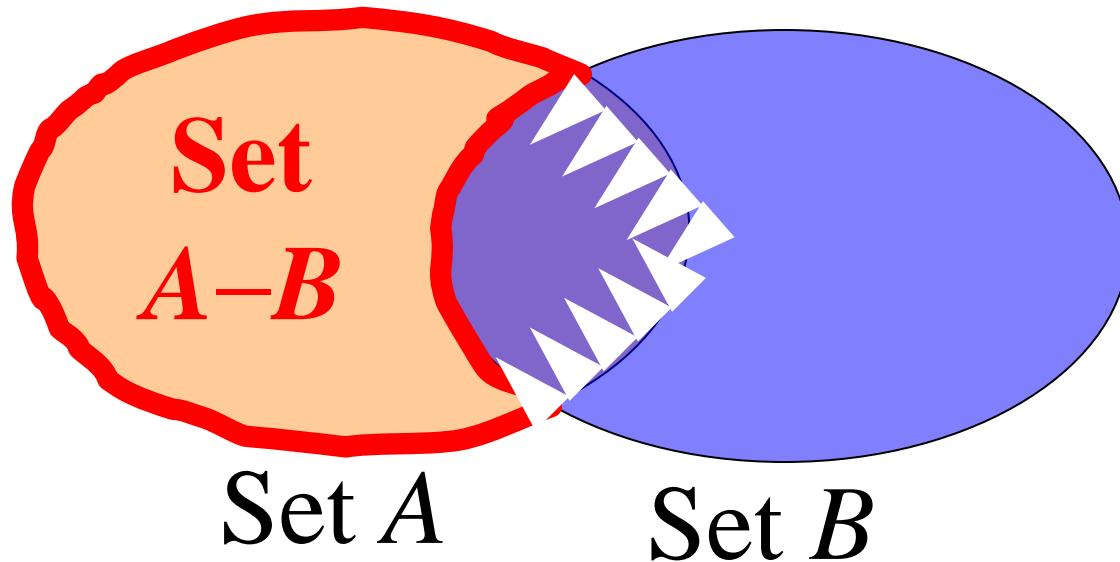
Set Difference Examples

- $\{1, 2, 3, 4, 5, 6\} - \{2, 3, 5, 7, 9, 11\} = \{1, 4, 6\}$ 

The diagram illustrates the set difference operation. It shows two sets: $\{1, 2, 3, 4, 5, 6\}$ and $\{2, 3, 5, 7, 9, 11\}$. Red arrows point from the elements 2, 3, and 5 in the first set to the second set, indicating they are being removed. The elements 1, 4, and 6 remain in the first set, which is the result of the set difference.
- $\mathbb{Z} - \mathbb{N} =$
$$= \{\dots, -1, 0, 1, 2, \dots\} - \{0, 1, \dots\}$$
$$= \{x \mid x \text{ is an integer but not a Natural.}\}$$
$$= \{x \mid x \text{ is a negative integer}\}$$
$$= \{\dots, -3, -2, -1\}$$

Set Difference – Venn Diagram

- $A - B$ is what's left after B
“takes a bite out of A ”



Set Complements

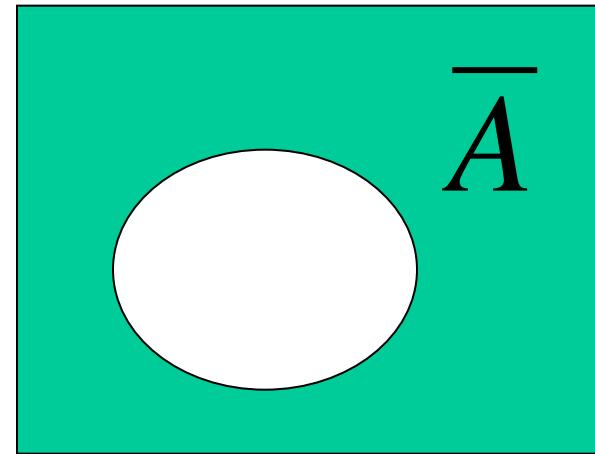
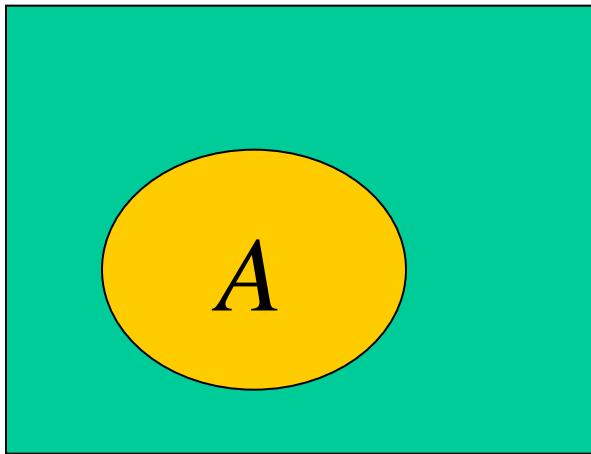
- The universe of discourse can itself be considered a set, call it U .
- When the context clearly defines U , we say that for any set $A \subseteq U$, the complement of A , written \bar{A} , is the complement of A w.r.t. U , i.e., it is $U - A$.
- E.g., If $U = \mathbb{N}$, $\overline{\{3,5\}} = \{0,1,2,4,6,7, \dots\}$

More on Set Complements

- An equivalent definition, when U is clear:

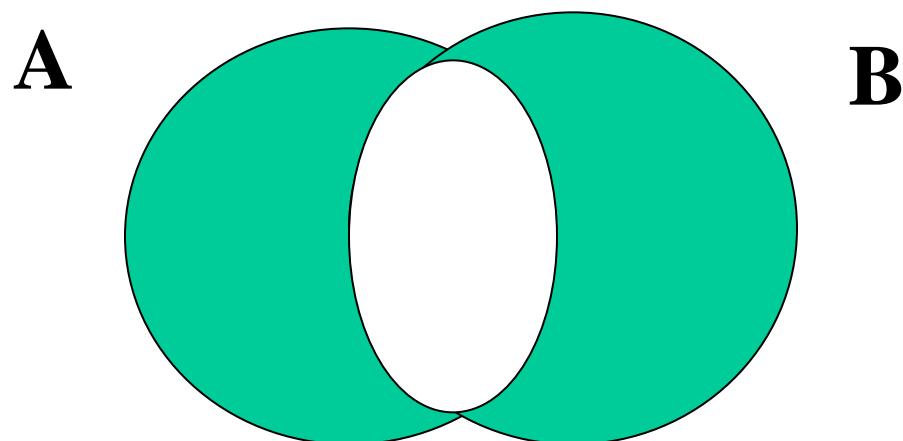
$$\overline{A} = \{x \mid x \notin A\}$$

U



Symmetric difference

- $A \oplus B = (A - B) \cup (B - A)$



Cardinality

- $|P \cup Q| = |P| + |Q| - |P \cap Q|$
- $|P \oplus Q| = |P| + |Q| - 2|P \cap Q|$
- $|P - Q| = |P| - |P \cap Q|$
- $|\bar{A}| = |U| - |A|$, U is universe of discourse

Set Identities

- Identity:

$$A \cup \emptyset = A, \quad A \cap U = A$$

- Domination:

$$A \cup U = U, \quad A \cap \emptyset = \emptyset$$

- Idempotent:

$$A \cup A = A = A \cap A$$

Set Identities

- Double complement:

$$\overline{\overline{A}} = A$$

- Commutative:

$$A \cup B = B \cup A, \quad A \cap B = B \cap A$$

- Associative:

$$A \cup (B \cup C) = (A \cup B) \cup C$$

$$A \cap (B \cap C) = (A \cap B) \cap C$$

DeMorgan's Law for Sets

- Exactly analogous to (and derivable from) DeMorgan's Law for propositions.

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Proving Set Identities

To prove statements about sets, of the form $E_1 = E_2$ (where E s are set expressions), here are three useful techniques:

1. Prove $E_1 \subseteq E_2$ and $E_2 \subseteq E_1$ separately.
2. Use set builder notation & logical equivalences.
3. Use a membership table.

Method 1: Mutual subsets

Example: Show $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

- Show $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.
 - Assume $x \in A \cap (B \cup C)$, & show $x \in (A \cap B) \cup (A \cap C)$.
 - We know that $x \in A$, and either $x \in B$ or $x \in C$.
 - Case 1: $x \in B$. Then $x \in A \cap B$, so
 $x \in (A \cap B) \cup (A \cap C)$.
 - Case 2: $x \in C$. Then $x \in A \cap C$, so
 $x \in (A \cap B) \cup (A \cap C)$.
 - Therefore, $x \in (A \cap B) \cup (A \cap C)$.
 - Therefore, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.
 - Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ Homework.

Method 3: Membership Tables

- Just like truth tables for propositional logic.
- Columns for different set expressions.
- Rows for all combinations of memberships in constituent sets.
- Use “1” to indicate membership in the derived set, “0” for non-membership.
- Prove equivalence with identical columns.

Membership Table Example

Example: Prove $(A \cup B) - B = A - B$.

A	B	$A \cup B$	$(A \cup B) - B$	$A - B$
0	0	0	0	0
0	1	1	0	0
1	0	1	1	1
1	1	1	0	0

Membership Table Exercise

Exercise: Prove $(A \cup B) - C = (A - C) \cup (B - C)$.

A	B	C	$A \cup B$	$(A \cup B) - C$	$A - C$	$B - C$	$(A - C) \cup (B - C)$
0	0	0					
0	0	1					
0	1	0					
0	1	1					
1	0	0					
1	0	1					
1	1	0					
1	1	1					

Generalized Unions & Intersections

- Since union & intersection are commutative and associative, we can extend them from operating on ordered pairs of sets (A, B) to operating on sequences of sets (A_1, \dots, A_n) , or even unordered sets of sets, $X = \{A \mid P(A)\}$.

Generalized Union

- Binary union operator: $A \cup B$
- n-ary union:
$$A_1 \cup A_2 \cup \dots \cup A_n := (((\dots((A_1 \cup A_2) \cup \dots) \cup A_n)$$

(grouping & order is irrelevant)

- “Big U” notation:
$$\bigcup_{i=1}^n A_i$$
- Or for infinite sets of sets:
$$\bigcup_{A \in X} A$$

Generalized Intersection

- Binary intersection operator: $A \cap B$
- n-ary intersection:
$$A_1 \cap A_2 \cap \dots \cap A_n := (((\dots((A_1 \cap A_2) \cap \dots) \cap A_n)$$

(grouping & order is irrelevant)

- “Big Arch” notation: $\bigcap_{i=1}^n A_i$
- Or for infinite sets of sets: $\bigcap_{A \in X} A$

Representations

- A frequent theme of this course will be methods of representing one discrete structure using another discrete structure of a different type.
- E.g., one can represent natural numbers as
 - Sets:
 $0 := \emptyset, 1 := \{0\}, 2 := \{0,1\}, 3 := \{0,1,2\}, \dots$
 - Bit strings:
 $0 := 0, 1 := 1, 2 := 10, 3 := 11, 4 := 100, \dots$

Representing Sets with Bit Strings

For an enumerable u.d. U with ordering $\{x_1, x_2, \dots, x_n\}$, represent a finite set $S \subseteq U$ as the finite bit string $B = b_1 b_2 \dots b_n$ where $\forall i: x_i \in S \leftrightarrow (i < n \wedge b_i = 1)$.

E.g. $U = \mathbb{N}$, $S = \{2, 3, 5, 7, 11\}$,
 $B = 001101010001$.

In this representation, the set operators “ \cup ”, “ \cap ”, “ $^{-}$ ” are implemented directly by bitwise OR, AND, NOT!

TABLE 1 Set Identities.

<i>Identity</i>	<i>Name</i>
$A \cap U = A$ $A \cup \emptyset = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws

TABLE 1 Set Identities.

<i>Identity</i>	<i>Name</i>
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

The **symmetric difference** of A and B , denoted by $A \oplus B$, is the set containing those elements in either A or B , but not in both A and B .

Find the symmetric difference of $\{1, 3, 5\}$ and $\{1, 2, 3\}$.

Show that $A \oplus B = (A \cup B) - (A \cap B)$.

Show that $A \oplus B = (A - B) \cup (B - A)$.

Show that if A is a subset of a universal set U , then

- a) $A \oplus A = \emptyset$.
- b) $A \oplus \emptyset = A$.
- c) $A \oplus U = \overline{A}$.
- d) $A \oplus \overline{A} = U$.

Example: Show that $A \oplus B = (A \cup B) - (A \cap B)$.

Example: Show that $A \oplus B = (A \cup B) - (A \cap B)$.

element is in $(A \cup B) - (A \cap B)$ if it is in the union of A and B but not in the intersection of A and B , which means that it is in either A or B but not in both A and B . This is exactly what it means for an element to belong to $A \oplus B$.

Example: Show that if A is a subset of a universal set U , then

a) $A \oplus A = \emptyset.$

c) $A \oplus U = \overline{A}.$

b) $A \oplus \emptyset = A.$

d) $A \oplus \overline{A} = U.$

Example: Show that if A is a subset of a universal set U , then

a) $A \oplus A = \emptyset.$

b) $A \oplus \emptyset = A.$

c) $A \oplus U = \overline{A}.$

d) $A \oplus \overline{A} = U.$

a) $A \oplus A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$

Example: Show that if A is a subset of a universal set U , then

a) $A \oplus A = \emptyset.$

b) $A \oplus \emptyset = A.$

c) $A \oplus U = \overline{A}.$

d) $A \oplus \overline{A} = U.$

a) $A \oplus A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$

b) $A \oplus \emptyset = (A - \emptyset) \cup (\emptyset - A) = A \cup \emptyset = A$

Example: Show that if A is a subset of a universal set U , then

a) $A \oplus A = \emptyset.$

b) $A \oplus \emptyset = A.$

c) $A \oplus U = \overline{A}.$

d) $A \oplus \overline{A} = U.$

a) $A \oplus A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$

b) $A \oplus \emptyset = (A - \emptyset) \cup (\emptyset - A) = A \cup \emptyset = A$

c) $A \oplus U = (A - U) \cup (U - A) = \emptyset \cup \overline{A} = \overline{A}$

Example: Show that if A is a subset of a universal set U , then

a) $A \oplus A = \emptyset.$

b) $A \oplus \emptyset = A.$

c) $A \oplus U = \overline{A}.$

d) $A \oplus \overline{A} = U.$

a) $A \oplus A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$

b) $A \oplus \emptyset = (A - \emptyset) \cup (\emptyset - A) = A \cup \emptyset = A$

c) $A \oplus U = (A - U) \cup (U - A) = \emptyset \cup \overline{A} = \overline{A}$

d) $A \oplus \overline{A} = (A - \overline{A}) \cup (\overline{A} - A) = A \cup \overline{A} = U$

Examples: $U = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$A = \{1, 2, 3, 4, 5\}$, $B = \{4, 5, 6, 7, 8\}$. Then

- $A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8\}$
- $A \cap B = \{4, 5\}$
- $\overline{A} = \{0, 6, 7, 8, 9, 10\}$
- $\overline{B} = \{0, 1, 2, 3, 9, 10\}$
- $A - B = \{1, 2, 3\}$
- $B - A = \{6, 7, 8\}$
- $A \oplus B = \{1, 2, 3, 6, 7, 8\}$

Mat2033 - Discrete Mathematics

Relations and their Properties

A binary relation from A to B is a subset of $A \times B$

- The Cartesian product of two sets, say A and B
- We might represent this as a set of ordered pairs
- In a pair, first is from A, second is from B

The relation is a set of pairs where first element is from A and second is from B

$$a \in A \wedge b \in B$$

We say "*a is related to b by R*" where R is a relation

$$a R b \Leftrightarrow (a, b) \in R$$

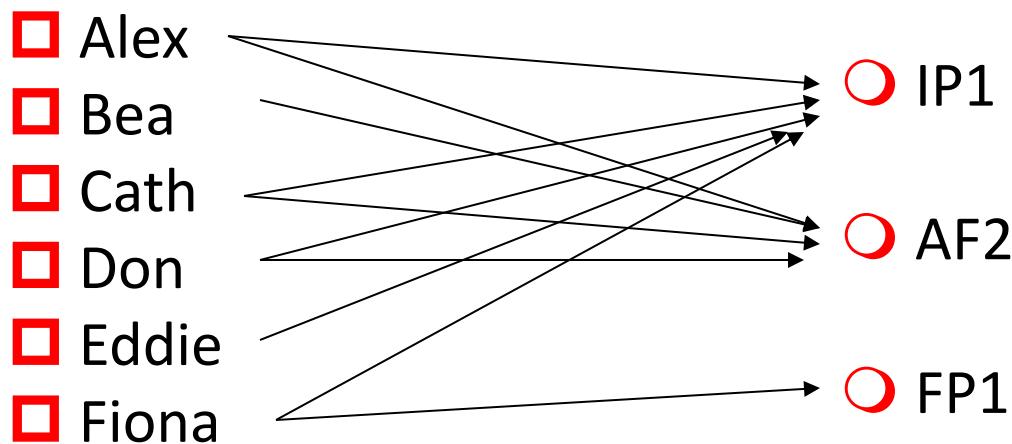
- Students:
 - Alex, Bea, Cath, Don, Eddie, Fiona
- Subjects:
 - IP1, FP1, AF2
- Let R be the relation of students who passed subjects

$$R = \{(Alex, IP1), (Alex, AF2), (Bea, AF2), (Cath, AF2), (Cath, IP1), (Don, AF2), (Don, IP1), (Fiona, IP1), (Eddie, IP1), (Fiona, FP2)\}$$

Order between pairs is insignificant (look at Fiona)

R is a set. Right?

Order within pairs ***is*** significant (a pair (FP2,Fiona)?)

$$R = \{(Alex, IP1), (Alex, AF2), (Bea, AF2), (Cath, AF2), (Cath, IP1), (Don, AF2), (Don, IP1), (Fiona, IP1), (Eddie, IP1), (Fiona, FP1)\}$$


But you could have functional relations

It isn't a function!

Example: How many relations are there on a set of n elements?

- Each relation R_i is a subset of $\{(a,b) \mid a \in A \wedge b \in B\}$
 R_i is a subset of the Cartesian product of A and B
 - When we have a relation on a single set, this is just $A = B$
 R_i is then a subset of $\{(x,y) \mid x \in A \wedge y \in A\}$
 - The cardinality of $A \times A$ is $|A \times A| = n^2$
 - There are 2^n subsets of a set of size n
 - If the set of tuples to choose from is of size n^2
then there are 2^{n^2} possible subsets
- ✓ There are $2^{(n^2)}$ possible relations

Equivalence Relations and Partitions

Now we take up an idea fundamental for computer science and mathematics. Indeed, you have seen equivalence relations from the beginning of your study of mathematics and computer science.

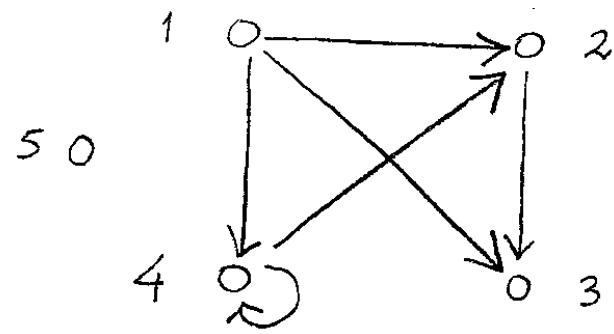
Relations, Graphs, and Matrices

Definition: A binary relation on a set A is a subset of the Cartesian product $A \times A$.

As you can see, the concept of relation is very general. Let us look at different ways to define a relation. We defined it as a set of ordered pairs. It can also be viewed as a directed graph or as a relation matrix.

The directed graph of the relation is the set of points of A together with the ordered pairs of the given relation; these two sets are often represented in a sketch as a set of dots, one dot for each point of A , and a set of arrows joining the dots, one arrow for each ordered pair (a,b) in the given relation, and drawn as an arrow from a to b :

Example: The relation $\{(1,2), (1,3), (1,4), (2,3), (4,4), (4,2)\}$ on the set $A = \{1, 2, 3, 4, 5\}$ has the graph



The arrow from "1" to "2" stands for the ordered pair $(1,2)$

The relation-matrix is a square array of 0's and 1's with rows and columns labeled by the elements of A , one row and one column for each such element. For each a, b in A , the entry in row a and column b of the matrix is 1 if (a, b) is one of the ordered pairs of the relation, and 0 if it is not.

	1	2	3	4	5
1	0	1	1	1	0
2	0	0	1	0	0
3	0	0	0	0	0
4	0	1	0	1	0
5	0	0	0	0	0

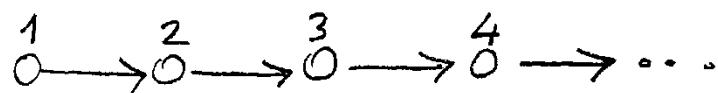
The relation-matrix
of the above example.

Example: The relation $\{(1, 2), (1, 3), (1, 4), (2, 3), (4, 4), (4, 2)\}$
on the set $A = \{1, 2, 3, 4, 5\}$,

Example: An example of a relation R defined by the set-builder notation

$$R = \{(a, b) \mid a, b \in \mathbb{N}, b = a+1\}$$

The graph of R is



Its relation-matrix is an infinite matrix that in its upper left corner is

	1	2	3	4	...
1	0	1	0	0	
2	0	0	1	0	...
3	0	0	0	1	
:	:				

Note: To convince you how general the idea of relation is, we now observe that our five-point set A of above example has a total of more than 32,000,000 different relations on it. Precisely, there are 2^{25} of them, because every different subset of the 25-point set $A \times A$ is a different relation. So we shall narrow our inquiry to a much smaller class of relations: the equivalence relations.

Equivalence Relations

Definition: A relation on a set A is called an equivalence relation if and only if it is reflexive, symmetric, and transitive.

Definition: A relation R is reflexive if and only if for all $a \in A$, (a, a) is in the relation R .

Thus in graphical terms, there must be a loop at every point of A . In the relation-matrix, the main diagonal must be all 1's.

Example: The prior examples are not reflexive.
The complete relation $R = A \times A$ on A is reflexive,
of course.

Practice: Prove $R' = \{(x, y) \mid x, y \in \mathbb{N}, x \leq y\}$ is reflexive.

Note: We can easily count the number of reflexive relations on our five-point set A . There are 2^{20} , about 1,000,000, of them. This is so because a reflexive relation R may be any subset of $A \times A$ that includes $D = \{(x, x) | x \in A\}$, a set of five points: $D \subseteq R \subseteq A \times A$.

Our answer is the total number of subsets of $(A \times A) - D$. This set has $25 - 5 = 20$ points and, therefore, 2^{20} subsets.

Example: Consider these relations on the set of integers:

$$R_1 = \{(a, b) \mid a \leq b\},$$

$$R_2 = \{(a, b) \mid a > b\},$$

$$R_3 = \{(a, b) \mid a = b \text{ or } a = -b\},$$

$$R_4 = \{(a, b) \mid a = b\},$$

$$R_5 = \{(a, b) \mid a = b + 1\},$$

$$R_6 = \{(a, b) \mid a + b \leq 3\}.$$

Which of these relations are reflexive?

Solution: The reflexive relations from Example 5 are R_1 (because $a \leq a$ for every integer a), R_3 , and R_4 . For each of the other relations in this example it is easy to find a pair of the form (a, a) that is not in the relation. (This is left as an exercise for the reader.) ◀

Definition: A relation R is symmetric if and only if, for every ordered pair (a,b) in R , the reversed ordered pair (b,a) is also in R .

* Thus whenever we have one arrow in the graph, there must be another arrow "going backward" (except for loops, of course). The relation-matrix must be symmetric about the main diagonal.

Examples: Consider $R = \mathbb{A} \times \mathbb{A}$ again, the complete relation. It is symmetric, of course. Its relation-matrix consists entirely of 1's.

Define now R' on \mathbb{N} as

$$R' = \{(a,b) \mid a, b \in \mathbb{N}, a+b \text{ is odd}\}$$

Definition: A relation R is symmetric if and only if, for every ordered pair (a,b) in R , the reversed ordered pair (b,a) is also in R .

* Thus whenever we have one arrow in the graph, there must be another arrow "going backward" (except for loops, of course). The relation-matrix must be symmetric about the main diagonal.

Examples: Consider $R = \mathbb{A} \times \mathbb{A}$ again, the complete relation. It is symmetric, of course. Its relation-matrix consists entirely of 1's.

Define now R' on \mathbb{N} as

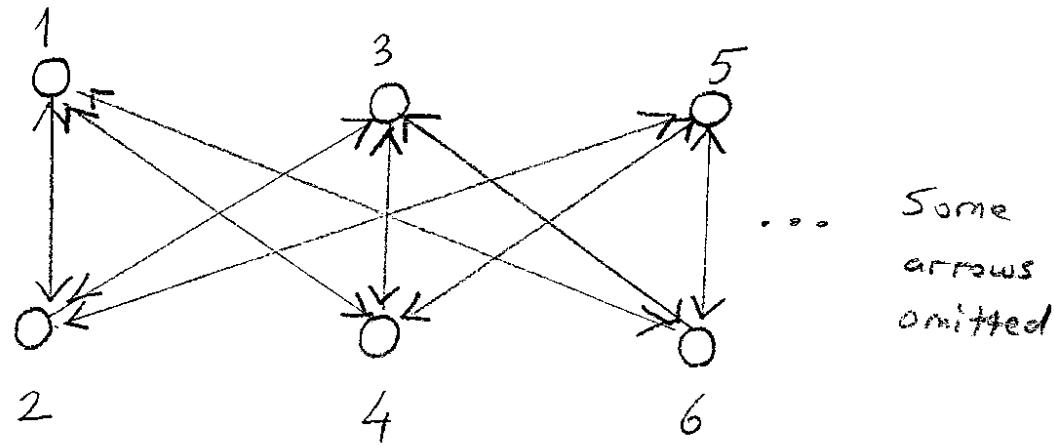
$$R' = \{(a,b) \mid a, b \in \mathbb{N}, a+b \text{ is odd}\}$$

Thus two integers are related by R' iff one is even and the other is odd. R' is symmetric. The upper left corner of the relation-matrix of R' is

	1	2	3	4	...
1	0	1	0	1	
2	1	0	1	0	...
3	0	1	0	1	
:	:				

You can see in various ways that R' is not reflexive.

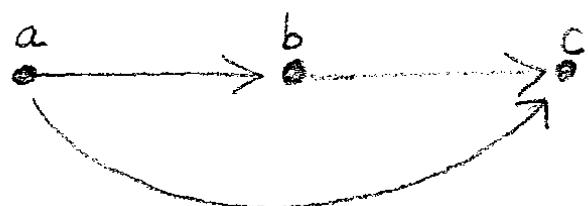
The graph of R' is, in part



There are too many arrows to draw here. They exist in both directions between each odd and each even integer.

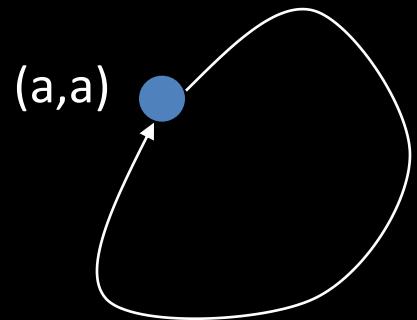
Definition: A relation R is transitive if and only if, for all a, b, c in A [$(a, b) \in R$ and $(b, c) \in R$] implies $(a, c) \in R$

In a graph of R this property tells of certain shortcuts: whenever we can go from a to c in two steps, we can go there in one step.



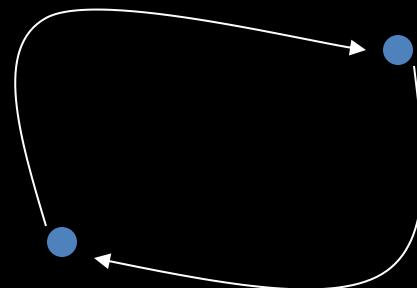
- Reflexive:
 - if a is in A then (a,a) is in R
- Symmetric:
 - if (a,b) is in R and $a \neq b$ then (b,a) is in R
- Antisymmetric:
 - if (a,b) is in R and $a \neq b$ then (b,a) is not in R
- Transitive:
 - if (a,b) is in R and (b,c) is in R then (a,c) is in R

- Reflexive
 - if a is in A then (a,a) is in R
- Example: a divides b i.e. $a|b$
 - $R = \{(a,b) \mid a \in A, b \in B, a|b\}$



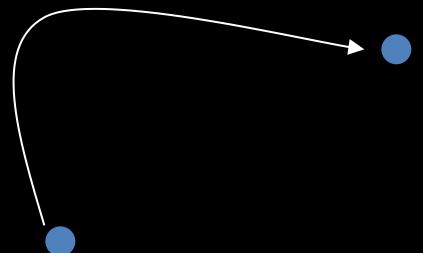
$$a \in A \rightarrow (a, a) \in R$$

- Symmetric
 - if (a,b) is in R and $a \neq b$
then (b,a) is in R



Example: a is married to b

$$(a,b) \in R \wedge a \neq b \rightarrow (b,a) \in R$$



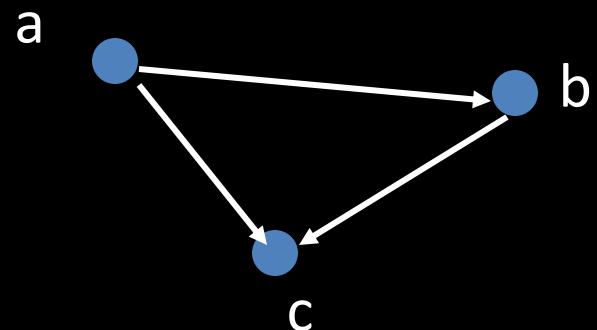
- Antisymmetric
 - if (a,b) is in R and $a \neq b$
then (b,a) is not in R

Example: a divides b i.e. $a|b$ and $a < b$

$$R = \{(a,b) \mid a \text{ in } A, b \text{ in } B, a|b\}$$

$$(a,b) \in R \wedge a \neq b \rightarrow (b,a) \notin R$$

- Transitive
 - if (a,b) is in R and (b,c) is in R
then (a,c) is in R



Example: a is less than b i.e. $a < b$

- a and b are positive integers
- $R = \{(a,b) \mid a < b\}$

$$(a,b) \in R \wedge (b,c) \in R \rightarrow (a,c) \in R$$

Exercise:

Consider the following relations on $\{1, 2, 3, 4\}$:

$$R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\},$$

$$R_2 = \{(1, 1), (1, 2), (2, 1)\},$$

$$R_3 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\},$$

$$R_4 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\},$$

$$R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\},$$

$$R_6 = \{(3, 4)\}.$$

Exercise: Consider these relations on the set of integers:

$$R_1 = \{(a, b) \mid a \leq b\},$$

$$R_2 = \{(a, b) \mid a > b\},$$

$$R_3 = \{(a, b) \mid a = b \text{ or } a = -b\},$$

$$R_4 = \{(a, b) \mid a = b\},$$

$$R_5 = \{(a, b) \mid a = b + 1\},$$

$$R_6 = \{(a, b) \mid a + b \leq 3\}.$$

$$A = \{1, 2, 3\} \quad B = \{1, 2, 3, 4\}$$

$$R_1 = \{(1,1), (2,2), (3,3)\}$$

$$R_2 = \{(1,1), (1,2), (1,3), (1,4)\}$$

$$R_1 \cup R_2 = \{(1,1), (1,2), (2,2), (1,3), (1,4), (3,3)\}$$

$$R_1 \cap R_2 = \{(1,1)\}$$

$$R_1 - R_2 = \{(2,2), (3,3)\}$$

$$R_2 - R_1 = \{(1,2), (1,3), (1,4)\}$$

Let R_1 be the “less than” relation on the set of real numbers and let R_2 be the “greater than” relation on the set of real numbers, that is, $R_1 = \{(x, y) \mid x < y\}$ and $R_2 = \{(x, y) \mid x > y\}$. What are $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 - R_2$, $R_2 - R_1$, and $R_1 \oplus R_2$?

Let R_1 be the “less than” relation on the set of real numbers and let R_2 be the “greater than” relation on the set of real numbers, that is, $R_1 = \{(x, y) \mid x < y\}$ and $R_2 = \{(x, y) \mid x > y\}$. What are $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 - R_2$, $R_2 - R_1$, and $R_1 \oplus R_2$?

Solution: We note that $(x, y) \in R_1 \cup R_2$ if and only if $(x, y) \in R_1$ or $(x, y) \in R_2$. Hence, $(x, y) \in R_1 \cup R_2$ if and only if $x < y$ or $x > y$. Because the condition $x < y$ or $x > y$ is the same as the condition $x \neq y$, it follows that $R_1 \cup R_2 = \{(x, y) \mid x \neq y\}$. In other words, the union of the “less than” relation and the “greater than” relation is the “not equals” relation.

Next, note that it is impossible for a pair (x, y) to belong to both R_1 and R_2 because it is impossible for $x < y$ and $x > y$. It follows that $R_1 \cap R_2 = \emptyset$. We also see that $R_1 - R_2 = R_1$, $R_2 - R_1 = R_2$, and $R_1 \oplus R_2 = R_1 \cup R_2 - R_1 \cap R_2 = \{(x, y) \mid x \neq y\}$. ◀

- ▶ Let R be a relation from set A to set B
- ▶ Let S be a relation from set B to set C
- ▶ The composite of R and S is a relation from set A to set C
 - ▶ and is a set of ordered pairs (a,c) such that
 - ▶ there exists an (a,b) in R and an (b,c) in S
- ▶ The composite of R and S is denoted as $S \circ R$

The composite of R with S

$S \circ R$

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

$$S = \{(1,0), (2,0), (3,1), (3,2), (4,1)\}$$

$$S \circ R = \{(1,0), (1,1), (2,1), (2,2), (3,0), (3,1)\}$$

Mat2033 - Discrete Mathematics

Relations and their Properties
Continue...

- ▶ Let R be a relation from set A to set B
- ▶ Let S be a relation from set B to set C
- ▶ The composite of R and S is a relation from set A to set C
 - ▶ and is a set of ordered pairs (a,c) such that
 - ▶ there exists an (a,b) in R and an (b,c) in S
- ▶ The composite of R and S is denoted as $S \circ R$

The composite of R with S

$S \circ R$

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

$$S = \{(1,0), (2,0), (3,1), (3,2), (4,1)\}$$

$$S \circ R = \{(1,0), (1,1), (2,1), (2,2), (3,0), (3,1)\}$$

Assume we have a relation R of people to motorcycles they own.

A person could have more than one motorcycle.

R is a set of ordered pairs $\{(Patrick, RGV), (Denis, Buell), (Stan, ElectraGlide), (Denis, Hayabusa), (Gordon, Bandit), (Gordon, R6)\}$

We could have a relation S of motorcycles to top speed

$\{(RGV, 130), (Buell, 126), (ElectraGlide, 110), (Hayabusa, 182), (Bandit, 140), (R6, 155)\}$

So R is then the relation of people to possible top speeds
 $\{(Patrick, 130), (Denis, 126), (Denis, 182), (Stan, 110), (Gordon, 140), (Gordon, 155)\}$

Composite of a Relation with itself

Let R be a relation on the set A . The powers R^n are defined inductively as follows

$$R^1 = R$$

$$R^n = R^{n-1} \circ R$$

$$\therefore R^2 = R^1 \circ R = R \circ R$$

$$\therefore R^3 = R^2 \circ R$$

Composite of a Relation with itself

$$R^1 = R$$

$$R^n = R^{n-1} \circ R$$

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

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

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

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

$$\therefore R^n = R^3$$

A Transitive Relation

Theorem: A relation R on a set A is transitive iff R^n is a subset of R for $n = 1, 2, 3, \dots$

Assume : $R^2 \subseteq R$

$(a,b) \in R \wedge (b,c) \in R \rightarrow (a,c) \in R^2$ // by definition of composition

$\therefore (a,c) \in R^2$

$(a,c) \in R^2 \wedge R^2 \subseteq R \rightarrow (a,c) \in R$

$\therefore \text{transitive}(R)$

The inductive step

Assume : $R^n \subseteq R$ // The inductive hypothesis

Show : $R^{n+1} \subseteq R$

Assume : $(a,b) \in R^{n+1}$

$R^{n+1} = R^n \circ R$ // Definition of composition

$\exists x(x \in A \wedge (a,x) \in R \wedge (x,b) \in R^n)$

$R^n \subseteq R \rightarrow (x,b) \in R$ // Using the inductive hypothesis

Since $\text{transitive}(R) \wedge (a,x) \in R \wedge (x,b) \in R \rightarrow (a,b) \in R$

$\therefore R^{n+1} \subseteq R$

Q.E.D

Example:

$$A = \{1, 2, 3, 4\}$$

$$R = \{(a, b) \mid a \text{ divides } b\}$$

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

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

RoR is a subset of R, therefore transitive

Obvious! If a divides b and b divides c then a divides c !

Exercise:

Let R be a relation on people such that (a,b) is “ a is a parent of b ”

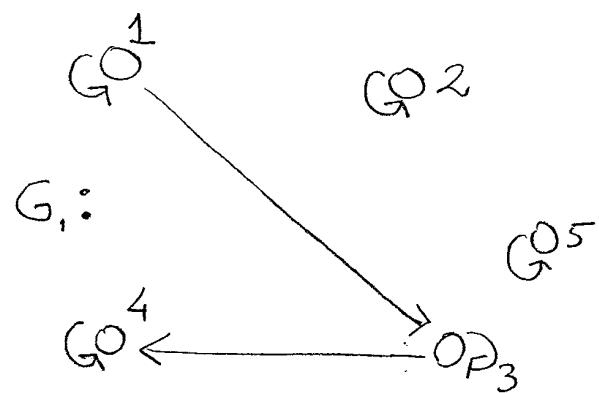
Let S be a relation on people such that (a,b) is “ a is a sibling of b ”

- What is SoR , RoS , RoR ?
 - SoR composes R with S
 - (a,c) is in SoR if there exists
 - (a,b) in R and a (b,c) in S
 - “ a is parent of b ” and “ b is sibling of c ”
 - SoR should be in R !
 - RoS composes S with R
 - “ a is sibling of b ” and “ b is a parent of c ”
 - therefore (a,c) is “ a is an aunt/uncle of c ”

Here are a few examples of relations with (or without) these properties, all on the set $A = \{1, 2, 3, 4, 5\}$. We denote the relation by R ; thus R is a set of ordered pairs from A . The graph we call G , and the matrix M , with rows and columns are labeled as before.

Example: , $R_1 = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,3), (3,4)\}$

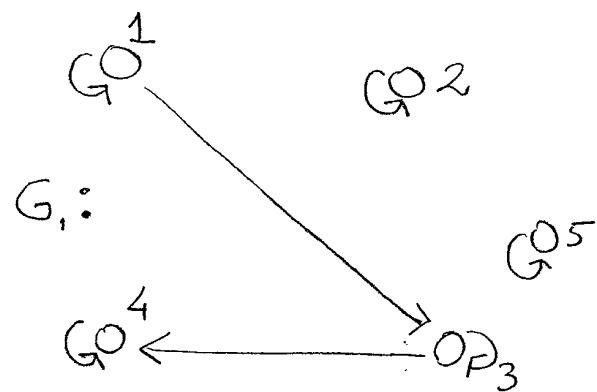
Example: , $R_1 = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,3), (3,4)\}$



	1	2	3	4	5
1	1	0	1	0	0
2	0	1	0	0	0
3	0	0	1	1	0
4	0	0	0	1	0
5	0	0	0	0	1

Example: , $R_1 = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,3), (3,4)\}$

A reflexive but not symmetric and not transitive relation, $R_1 = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,3), (3,4)\}$



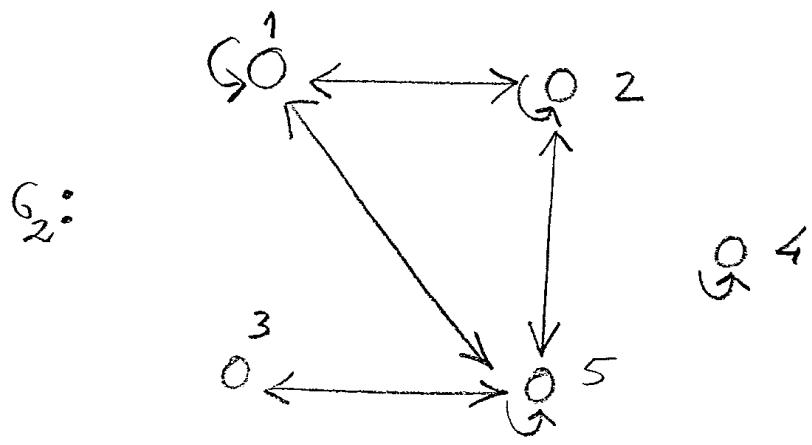
$M_1:$

	1	2	3	4	5
1	1	0	1	0	0
2	0	1	0	0	0
3	0	0	1	1	0
4	0	0	0	1	0
5	0	0	0	0	1

The presence of all the ordered pairs of the form (a,a) in R_1 is the requirement of the definition of reflexivity. We can also see that R_1 is reflexive by noting that there is a loop at every point of the graph G_1 , or that the main diagonal of M_1 consists entirely of 1's. R_1 is not symmetric because $(1,3) \in R_1$, but $(3,1) \notin R_1$. In G_1 there is no backward arrow to correspond to the arrow from 1 to 3; the matrix M_1 is not symmetric about the main diagonal. Since $(1,3)$ and $(3,4)$ are in R_1 , but $(1,4)$ is not in R_1 , it is not transitive.

Example : Let $R_2 = \{(1,1), (1,2), (1,5), (2,1), (2,2), (2,5), (3,5), (4,4), (5,1), (5,2), (5,3), (5,5)\}$.

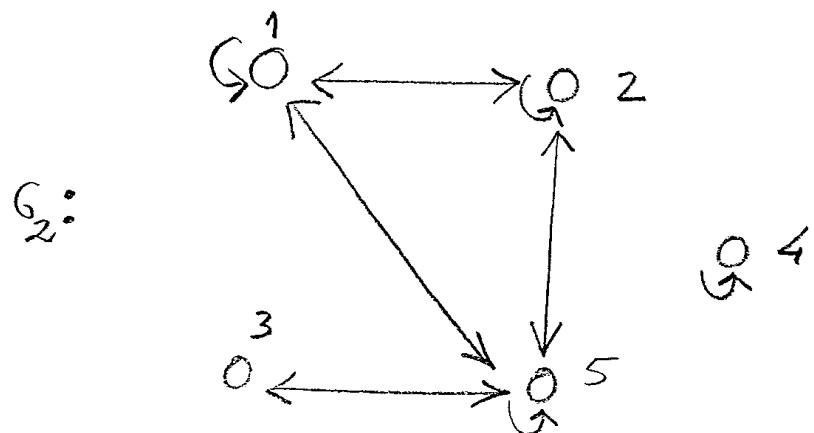
Example: Let $R_2 = \{(1,1), (1,2), (1,5), (2,1), (2,2), (2,5), (3,5), (4,4), (5,1), (5,2), (5,3), (5,5)\}$.



$$M_2: \begin{matrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{matrix}$$

Example: Let $R_2 = \{(1,1), (1,2), (1,5), (2,1), (2,2), (2,5), (3,5), (4,4), (5,1), (5,2), (5,3), (5,5)\}$.

Then R_2 is symmetric but is neither reflexive nor transitive.



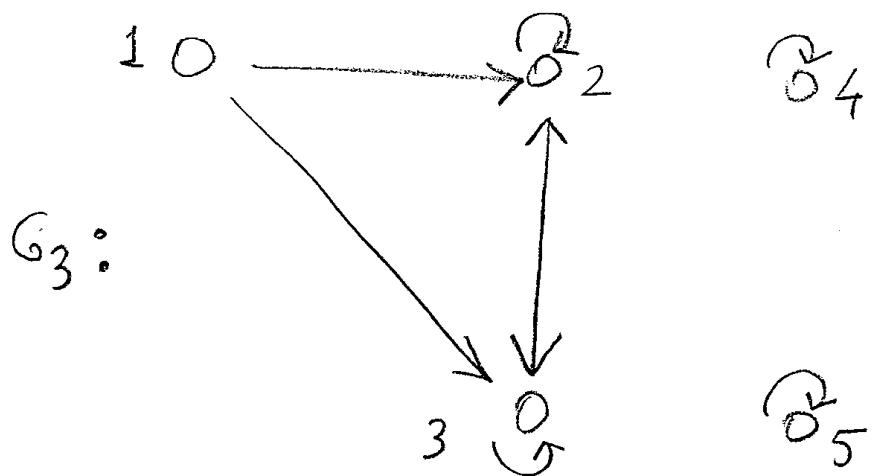
G_4

$$M_2: \begin{matrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{matrix}$$

In this example the symmetry is obvious from all three points of view. R_2 is not reflexive because $(3,3)$ is not in R_2 ; there is a '0' on the main diagonal. The nontransitivity is most apparent from the graph; there is a path from 3 to 5 to 1 but there is no shortcut from 3 to 1. Similarly for 3 and 2, and for the paths in the reverse directions.

Example: Take $R_3 = \{(1,2), (2,3), (1,3), (3,3), (4,4), (5,5), (2,2), (3,2)\}$

Example: Take $R_3 = \{(1,2), (2,3), (1,3), (3,3), (4,4), (5,5), (2,2), (3,2)\}$

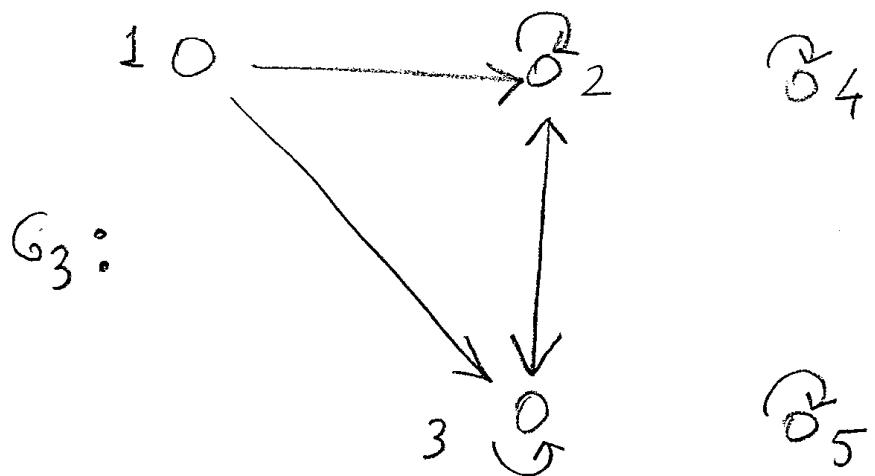


$M_3 :$

0	1	1		0
0	1	1		0
0	1	1		0
			1	0
			0	1

Example: Take $R_3 = \{(1,2), (2,3), (1,3), (3,3), (4,4), (5,5), (2,2), (3,2)\}$

R_3 is transitive but neither reflexive nor symmetric.



$M_3:$

0	1	1		0
0	1	1		0
0	1	1		0
			1	0
			0	1

A blank submatrix box, or one with a lone 0, is understood to have all its entries 0. Thus in M_3 the upper right and lower left corners are all 0. Reflexivity fails because (1,1) is not in R_3 ; the loop at 1 does not exist in G_3 ; there is a 0 on the main diagonal of M_3 . Symmetry fails because the back arrow is absent from 2 to 1 — for every arrow there must be a back arrow, or else the graph (relation) is not symmetric. Or you can simply notice that the matrix is not symmetric about the main diagonal.

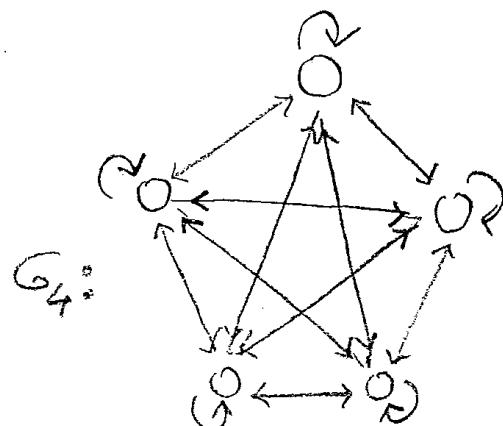
Now we discuss equivalence relations, those that are reflexive and symmetric and transitive.

Now we discuss equivalence relations, those that are reflexive and symmetric and transitive.

Example: $R_4 = A \times A$. For R_4 we have taken the set of all possible ordered pairs from the set A . Obviously R_4 is an equivalence relation. We show the graph G_4 and the matrix M_4 in the case that $A = \{1, 2, 3, 4, 5\}$

Now we discuss equivalence relations, those that are reflexive and symmetric and transitive.

Example: $R_4 = A \times A$. For R_4 we have taken the set of all possible ordered pairs from the set A . Obviously R_4 is an equivalence relation. We show the graph G_4 and the matrix M_4 in the case that $A = \{1, 2, 3, 4, 5\}$

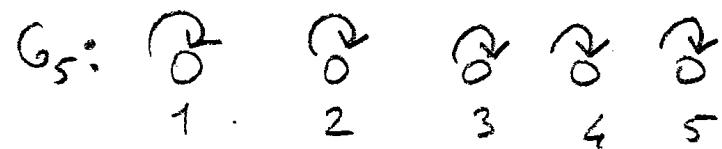


$$M_4 :$$

1	1	1	1	1
1	1	1	1	1
1	1	1	1	1
1	1	1	1	1

Example: Let $R_5 = \{(1,1), (2,2), (3,3), (4,4), (5,5)\}$. The graph and matrix are

Example: Let $R_5 = \{(1,1), (2,2), (3,3), (4,4), (5,5)\}$. The graph and matrix are

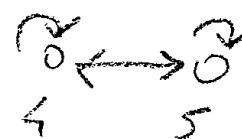
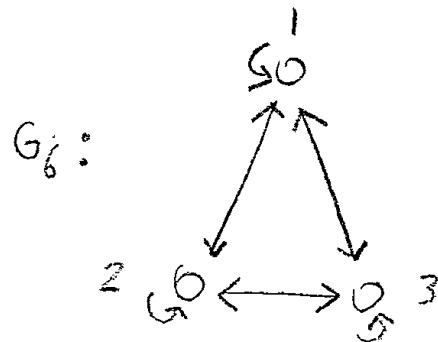


$$M_5: \begin{vmatrix} 1 & & & & \\ & 1 & 0 & & \\ & & 1 & & \\ 0 & & & 1 & \\ & & & & 1 \end{vmatrix}$$

This equivalence relation is the other extreme from R_4 . It is the smallest subset of $A \times A$ that is reflexive, symmetric and transitive.

Example: $R_6 = R_5 \cup \{(1,2), (2,1), (1,3), (3,1), (2,3), (3,2), (4,5), (5,4)\}$

Example: $R_6 = R_5 \cup \{(1,2), (2,1), (1,3), (3,1), (2,3), (3,2), (4,5), (5,4)\}$



$M_6:$

1	1	1	
1	1	1	
1	1	1	
		1	1

Blank box in the upper right means there are no arrows from any point of $\{1, 2, 3\}$ to any point of $\{4, 5\}$. Similarly, the blank box in the lower left means that there are no arrows from $\{4, 5\}$ to any of $1, 2, 3$.

Exercise:

Consider the following relations on $\{1, 2, 3, 4\}$:

$$R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\},$$

$$R_2 = \{(1, 1), (1, 2), (2, 1)\},$$

$$R_3 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\},$$

$$R_4 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\},$$

$$R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\},$$

$X = \{1, 2, 3, 4, 5, 6\}$. The relation R on X given by
 $R = \{(1,1), (1,3), (1,5), (3,1), (3,3), (3,5), (5,1), (5,3), (5,5),$
 $(2,2), (2,6), (6,2), (6,6), (4,4)\}$ ■

Let R be an equivalence relation on a set X . For each $a \in X$, let

$$[a] = \{x \in X \mid xRa\}$$

Then

Definition: Let R be an equivalence relation on a set X . The sets $[a]$ defined in the above are called the equivalence classes of X given by the relation R .

Theorem 1 :

Let R be an equivalence relation on a set A . These statements for elements a and b of A are equivalent:

- (i) aRb
- (ii) $[a] = [b]$
- (iii) $[a] \cap [b] \neq \emptyset$

Theorem 1 :

Let R be an equivalence relation on a set A . These statements for elements a and b of A are equivalent:

- (i) aRb
- (ii) $[a] = [b]$
- (iii) $[a] \cap [b] \neq \emptyset$

Proof: We first show that (i) implies (ii). Assume that aRb . We will prove that $[a] = [b]$ by showing $[a] \subseteq [b]$ and $[b] \subseteq [a]$. Suppose $c \in [a]$. Then aRc . Because aRb and R is symmetric, we know that bRa . Furthermore, because R is transitive and bRa and aRc , it follows that bRc . Hence, $c \in [b]$. This shows that $[a] \subseteq [b]$. The proof that $[b] \subseteq [a]$ is similar; it is left as an exercise for the reader.

Theorem 1 :

Let R be an equivalence relation on a set A . These statements for elements a and b of A are equivalent:

- (i) aRb
- (ii) $[a] = [b]$
- (iii) $[a] \cap [b] \neq \emptyset$

Proof: We first show that (i) implies (ii). Assume that aRb . We will prove that $[a] = [b]$ by showing $[a] \subseteq [b]$ and $[b] \subseteq [a]$. Suppose $c \in [a]$. Then aRc . Because aRb and R is symmetric, we know that bRc . Furthermore, because R is transitive and bRa and aRc , it follows that bRc . Hence, $c \in [b]$. This shows that $[a] \subseteq [b]$. The proof that $[b] \subseteq [a]$ is similar; it is left as an exercise for the reader.

Second, we will show that (ii) implies (iii). Assume that $[a] = [b]$. It follows that $[a] \cap [b] \neq \emptyset$ because $[a]$ is nonempty (because $a \in [a]$ because R is reflexive).

Theorem 1 :

Let R be an equivalence relation on a set A . These statements for elements a and b of A are equivalent:

- (i) aRb
- (ii) $[a] = [b]$
- (iii) $[a] \cap [b] \neq \emptyset$

Proof: We first show that (i) implies (ii). Assume that aRb . We will prove that $[a] = [b]$ by showing $[a] \subseteq [b]$ and $[b] \subseteq [a]$. Suppose $c \in [a]$. Then aRc . Because aRb and R is symmetric, we know that bRa . Furthermore, because R is transitive and bRa and aRc , it follows that bRc . Hence, $c \in [b]$. This shows that $[a] \subseteq [b]$. The proof that $[b] \subseteq [a]$ is similar; it is left as an exercise for the reader.

Second, we will show that (ii) implies (iii). Assume that $[a] = [b]$. It follows that $[a] \cap [b] \neq \emptyset$ because $[a]$ is nonempty (because $a \in [a]$ because R is reflexive).

Next, we will show that (iii) implies (i). Suppose that $[a] \cap [b] \neq \emptyset$. Then there is an element c with $c \in [a]$ and $c \in [b]$. In other words, aRc and bRc . By the symmetric property, cRb . Then by transitivity, because aRc and cRb , we have aRb .

Because (i) implies (ii), (ii) implies (iii), and (iii) implies (i), the three statements, (i), (ii), and (iii), are equivalent. \triangleleft

We are now in a position to show how an equivalence relation *partitions* a set. Let R be an equivalence relation on a set A . The union of the equivalence classes of R is all of A , because an element a of A is in its own equivalence class, namely, $[a]_R$. In other words,

$$\bigcup_{a \in A} [a]_R = A.$$

In addition, from Theorem 1, it follows that these equivalence classes are either equal or disjoint, so

$$[a]_R \cap [b]_R = \emptyset,$$

when $[a]_R \neq [b]_R$.

These two observations show that the equivalence classes form a partition of A , because they split A into disjoint subsets.

More precisely, a **partition** of a set S is a collection of disjoint nonempty subsets of S that have S as their union. In other words, the collection of subsets A_i , $i \in I$ (where I is an index set) forms a partition of S if and only if

$$A_i \neq \emptyset \text{ for } i \in I,$$

$$A_i \cap A_j = \emptyset \text{ when } i \neq j,$$

and

$$\bigcup_{i \in I} A_i = S.$$

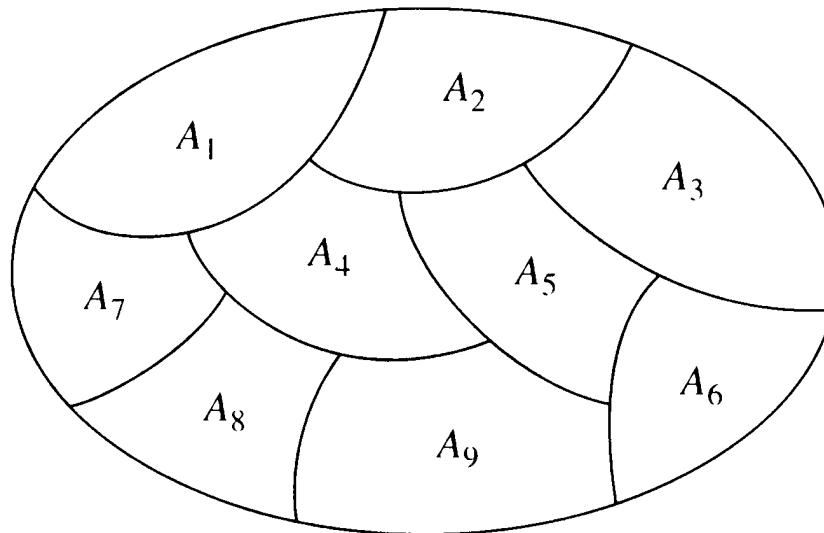


FIGURE 1 A Partition of a Set.

Partition of a set =

Suppose that we have a set X of 10 balls, each of which is either red, blue, or green

(B) R R G G

B R B G R

If we divide the balls into sets R, B , and G according to color, the family $\{R, B, G\}$ is a partition of X

A partition can be used to define a relation. If S is a partition of X , we may define xRy to mean that for some set $s \in S$, both x and y belong to s . For example the relation obtained could be described as "is the same color as". The next theorem shows that such a relation is always reflexive, symmetric, and transitive.

Theorem: Let \mathcal{S} be a partition of a set X . Define xRy to mean that for some set S in \mathcal{S} , both x and y belong to S . Then R is reflexive, symmetric, and transitive.

Proof: Let $x \in X$. By the definition of partition, x belongs to some member of $\mathcal{S} \subseteq \mathcal{S}$. Thus xRx and R is reflexive.

Suppose that xRy . Then both x and y belong to some set $S \in \mathcal{S}$. Since both y and x belong to S , yRx and R is symmetric.

Finally, suppose that xRy and yRz . Then both x and y belong to some set $S \in \mathcal{S}$ and both y and z belong to some set $T \in \mathcal{S}$. Since y belongs to exactly one member of \mathcal{S} , we must have $S=T$. Therefore, both x and z belong to S and xRz . We have shown that R is transitive.

Example: Consider the partition

$$S = \{\{1, 3, 5\}, \{2, 6\}, \{4\}\}$$

of $X = \{1, 2, 3, 4, 5, 6\}$. The relation R on X given by the above thm. contains the ordered pairs $(1, 1)$, $(1, 3)$, and $(1, 5)$; because $\{1, 3, 5\}$ is in S . The complete relation is

Example: Consider the partition

$$S = \{\{1, 3, 5\}, \{2, 6\}, \{4\}\}$$

of $X = \{1, 2, 3, 4, 5, 6\}$. The relation R on X given by the above thm. contains the ordered pairs $(1, 1)$, $(1, 3)$, and $(1, 5)$ because $\{1, 3, 5\}$ is in S . The complete relation is

$$R = \{(1, 1), (1, 3), (1, 5), (3, 1), (3, 3), (3, 5), (5, 1), (5, 3), (5, 5), (2, 2), (2, 6), (6, 2), (6, 6), (4, 4)\}.$$

Theorem: Let R be an equivalence relation on a set X . For each $a \in X$, let

$$[a] = \{x \in X \mid xRa\}$$

Then

$$S = \{[a] \mid a \in X\}$$

is a partition of X .

Proof: We must show that every element in X belongs to exactly one member of S .

Let $a \in X$. Since aRa , $a \in [a]$. Thus every element in X belongs to at least one member of S . It remains to show that every element in X belongs to exactly one member of S ; that is,

if $x \in X$ and $x \in [a] \cap [b]$, then $[a] = [b]$ (*)

We first show that if aRb , then $[a] = [b]$. Suppose that aRb . Let $x \in [a]$. Then xRa . Since aRb and R is transitive, xRb . Therefore, $x \in [b]$ and $[a] \subseteq [b]$. The argument that $[b] \subseteq [a]$ is the same as that just given, but with the roles of a and b interchanged. Thus $[a] = [b]$.

We now prove (*). Assume that $x \in X$ and $x \in [a] \cap [b]$. Then xRa and xRb . Our preceding result shows that $[x] = [a]$ and $[x] = [b]$. Thus $[a] = [b]$.

Example: Consider the partition

$$\mathcal{S} = \{\{1, 3, 5\}, \{2, 6\}, \{4\}\}$$

of $X = \{1, 2, 3, 4, 5, 6\}$. The equivalence class of $[1]$ containing 1 consists of all x such that $(x, 1) \in R$. Therefore,

$$[1] = \{1, 3, 5\}.$$

The remaining equivalence classes are found similarly:

$$[3] = [5] = \{1, 3, 5\},$$

$$[2] = [6] = \{2, 6\}$$

$$[4] = \{4\}.$$

Example: Let $X = \{1, 2, \dots, 10\}$. Define xRy to mean that 3 divides $x-y$. We can readily verify that the relation R is reflexive, symmetric, and transitive. Thus R is an equivalence relation on X .

Let us determine the members of the equivalence classes. The equivalence class $[1]$ consists of all x with $xR1$. Thus

$$[1] = \{x \in X \mid 3 \text{ divides } x-1\} = \{1, 4, 7, 10\}$$

Similarly,

$$[2] = \{2, 5, 8\}$$

$$[3] = \{3, 6, 9\}$$

These three sets partition X . Note that

$$[1] = [4] = [7] = [10]$$

$$[2] = [5] = [8]$$

$$[3] = [6] = [9].$$

Theorem: Let R be an equivalence relation on a finite set X . If each equivalence class has r elements, there are $|X|/r$ equivalence classes.

Proof: Let X_1, X_2, \dots, X_k denote the distinct equivalence classes. Since these sets partition X ,

$$|X| = |X_1| + |X_2| + \dots + |X_k| = r + r + \dots + r = kr$$

and the conclusion follows.

#1. Let R be the following relation defined on the set $\{a, b, c, d\}$:

$$R = \{(a,a), (a,c), (a,d), (b,a), (b,b), (b,c), (b,d), (c,b), (c,c), (d,b), (d,d)\}.$$

Determine whether R is:

Solution:

- (a) R is reflexive because R contains (a, a) , (b, b) , (c, c) , and (d, d) .
 - (b) R is not symmetric because $(a, c) \in R$, but $(c, a) \notin R$.
 - (c) R is not antisymmetric because both $(b, c) \in R$ and $(c, b) \in R$, but $b \neq c$.

Determine whether R is transitive.

Solution:

The relation R is not transitive because, for example, $(a, c) \in R$ and $(c, b) \in R$, but $(a, b) \notin R$.

- Floor Function: $\lfloor x \rfloor$ means take the greatest integer less than or equal to the number

Let n be an integer

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

Example:

$$\lfloor \frac{1}{2} \rfloor = 0$$

$$\lfloor -\frac{1}{2} \rfloor = -1$$

$$\lfloor 3.1 \rfloor = 3$$

$$\lfloor 7 \rfloor = 7$$

#2. Let R be the following relation on the set of real numbers:

$aRb \leftrightarrow \lfloor a \rfloor = \lfloor b \rfloor$, where $\lfloor x \rfloor$ is the floor of x .

Determine whether R is:

Solution:

(a) R is reflexive: $|a| = |a|$ is true for all real numbers.

(b) R is symmetric: suppose $|a| = |b|$; then $|b| = |a|$.

(c) R is not antisymmetric: we can have aRb and bRa for distinct a and b . For example, $|1.1| = |1.2|$.

Determine whether R is transitive.

Solution:

R is transitive: suppose $|a| = |b|$ and $|b| = |c|$; from transitivity of equality of real numbers, it follows that $|a| = |c|$.

#4. Let $A = \{(x, y) \mid x, y \text{ integers}\}$. Define a relation R on A by the rule

$$(a, b)R(c, d) \leftrightarrow a \leq c \text{ and } b \leq d.$$

Determine whether R is:

Solution:

(a) R is reflexive: $(a, b)R(a, b)$ for all elements (a, b) because $a \leq a$ and $b \leq b$ is always true.

(b) R is not symmetric: For example, $(1, 2)R(3, 7)$ (because $1 \leq 3$ and $2 \leq 7$), but $(3, 7)R(1, 2)$.

(c) R is antisymmetric: Suppose $(a, b)R(c, d)$ and $(c, d)R(a, b)$. Therefore $a \leq c$, $c \leq a$, $b \leq d$, $d \leq b$. Therefore $a = c$ and $b = d$, or $(a, b) = (c, d)$.

Determine whether R is transitive.

Solution:

R is transitive: Suppose $(a, b)R(c, d)$ and $(c, d)R(e, f)$. Therefore $a \leq c$ and $c \leq e$, and $b \leq d$ and $d \leq f$. Therefore, $a \leq e$ and $b \leq f$, or $(a, b)R(e, f)$.

#5. Let $A = \{(x, y) \mid x, y \text{ integers}\}$. Define a relation R on A by the rule

$$(a, b)R(c, d) \leftrightarrow a = c \text{ or } b = d.$$

Determine whether R is:

- (a) reflexive. (b) symmetric. (c) antisymmetric.

Solution:

- (a) R is reflexive: $(a, b)R(a, b)$ for all elements (a, b) because $a = a$ and $b = b$ are always true.
- (b) R is symmetric: Suppose $(a, b)R(c, d)$. Therefore $a = c$ or $b = d$. Therefore $c = a$ or $d = b$. Therefore $(c, d)R(a, b)$.
- (c) R is not antisymmetric: For example, $(1, 2)R(1, 3)$ and $(1, 3)R(1, 2)$ because $1 = 1$, but $(1, 2) \neq (1, 3)$.

Determine whether R is transitive.

Solution:

R is not transitive: For example, $(1, 2)R(1, 3)$ because $1 = 1$, and $(1, 3)R(4, 3)$ because $3 = 3$. But $(1, 2) \neq (4, 3)$ because $1 \neq 4$ and $2 \neq 3$.

#1. (a) Verify that the following is an equivalence relation on the set of real numbers:

$$aRb \leftrightarrow \lfloor a \rfloor = \lfloor b \rfloor, \text{ where } \lfloor x \rfloor \text{ is the floor of } x.$$

(b) Describe the equivalence classes arising from the equivalence relation in part (a).

Solution:

(a) R is reflexive: $\lfloor a \rfloor = \lfloor a \rfloor$ is true for all real numbers.

R is symmetric: suppose $\lfloor a \rfloor = \lfloor b \rfloor$; then $\lfloor b \rfloor = \lfloor a \rfloor$.

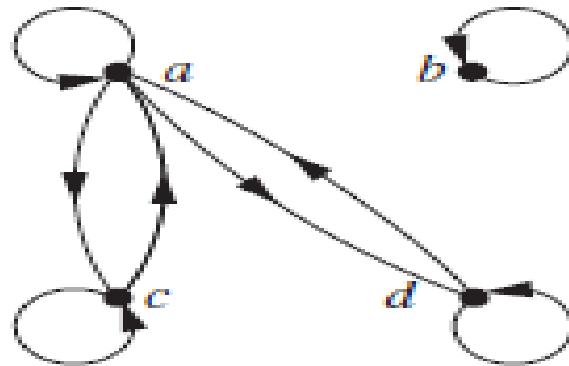
R is transitive: suppose $\lfloor a \rfloor = \lfloor b \rfloor$ and $\lfloor b \rfloor = \lfloor c \rfloor$; from transitivity of equality of real numbers, it follows that $\lfloor a \rfloor = \lfloor c \rfloor$.

(b) Two real numbers, a and b , are related if they have the same floor. This happens if and only if a and b lie in the same interval $[n, n + 1)$ where n is an integer. That is, the equivalence classes are the intervals $\dots, [-2, -1), [-1, 0), [0, 1), [1, 2), [2, 3), \dots$

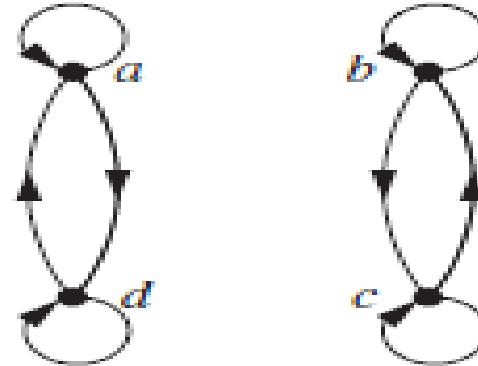
Exercise:

In Exercises 21–23 determine whether the relation with the directed graph shown is an equivalence relation.

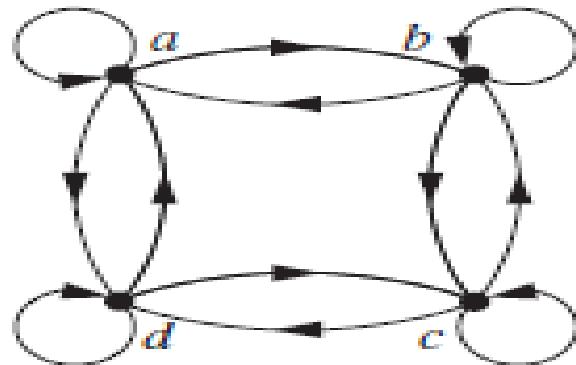
21.



22.



23.



Exercise:

24. Determine whether the relations represented by these zero-one matrices are equivalence relations.

a)
$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

b)
$$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

c)
$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Exercise:

Let R be the relation on the set of ordered pairs of positive integers such that $((a, b), (c, d)) \in R$ if and only if $a + d = b + c$. Show that R is an equivalence relation.

Exercise:

Let R be the relation on the set of ordered pairs of positive integers such that $((a, b), (c, d)) \in R$ if and only if $ad = bc$. Show that R is an equivalence relation.

Mat2033 - Discrete Mathematics

Partial Orderings

Definition 7.5. Relation R on the set S is called a **partial ordering** if it is reflexive, anti-symmetric and transitive. A set S together with a partial ordering R is called a **partially ordered set** (poset), denoted by (S, R) .

Example 7.8. Consider a relation on the set $S = \mathbb{R}$ defined as following:

$$R = \{(a, b) \in \mathbb{R} \times \mathbb{R} \mid a \leq b\}$$

Since for any real number a we have $a \leq a$, R is reflexive. For any real numbers a and b , if $a \leq b$ and $b \leq a$ then $a = b$. Therefore, R is anti-symmetric. For any real numbers a , b and c , if $a \leq b$ and $b \leq c$ then $a \leq c$. Therefore, R is transitive. So R is reflexive, anti-symmetric and transitive. Therefore, R is a partial ordering.

Example 7.9. Consider a relation on the set $S = \mathbb{N}$ defined as following:

$$R = \left\{ (a, b) \in \mathbb{N} \times \mathbb{N} \mid a|b \right\},$$

where $a|b$ means that a divides b .

Since for any natural number a we have $a|a$, R is reflexive. For any natural numbers a and b , if $a|b$ and $b|a$ then $a = b$. Therefore, R is anti-symmetric. For any natural numbers a , b and c , if $a|b$ and $b|c$ then $a|c$. Therefore, R is transitive. So R is reflexive, anti-symmetric and transitive. Therefore, R is a partial ordering.

Notation 7.1. Let (S, R) be any poset. For elements a and b of set S if $(a, b) \in R$ then we will say that ' a is less than or equal to b with respect to partial ordering R ' and will write $a \preceq b$. If $(a, b) \in R$ but $a \neq b$ then we will say that ' a is less than b with respect to partial ordering R ' and will write $a \prec b$.

Definition 7.6. Let (S, R) be a poset. The elements a and b of set S are called **comparable** with respect to partial ordering R if either $a \preceq b$ or $b \preceq a$. The elements a and b of set S are called **incomparable** with respect to partial ordering R if neither $a \preceq b$ nor $b \preceq a$.

Example 7.10. Consider again a relation

$$R = \left\{ (a, b) \in \mathbb{N} \times \mathbb{N} \mid a|b \right\}$$

which is a partial ordering on the set $S = \mathbb{N}$ (see Example 11.9). Natural numbers 7 and 28 are comparable with respect to partial ordering R and $7 \preceq 28$. Natural numbers 7 and 27 are incomparable with respect to R because neither $(7, 27) \in R$ nor $(27, 7) \in R$.

Definition 7.7. Let (S, R) be a poset. If every two elements a and b of set S are comparable with respect to partial ordering R then R is called a **total ordering** and S is called a **totally ordered set** with respect to R .

Example 7.11. Consider again a relation

$$R = \{(a, b) \in \mathbb{R} \times \mathbb{R} \mid a \leq b\}$$

which is a partial ordering on the set $S = \mathbb{R}$ (see Example 11.8). Since for any two real numbers a and b , we have either $a \leq b$ or $b \leq a$, this relation R is a total ordering.

Example 7.12. Obviously, a partial ordering

$$R = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a|b\}$$

is not a total ordering. (Why?)

Definition 7.8. Let R be a total ordering on the set S . Set S is called **well-ordered set** with respect to R if every nonempty subset of S has a least element.

Example 7.13. Consider a relation on the set $S = \mathbb{N}$ defined as following:

$$R = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a \leq b\}$$

which is a total ordering. Since any subset of \mathbb{N} has a least element, set \mathbb{N} is a well-ordered set with respect to this relation R .

Example 7.14. Now, consider a relation on the set $S = \mathbb{Z}$ defined as following:

$$R = \left\{ (a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \leq b \right\}$$

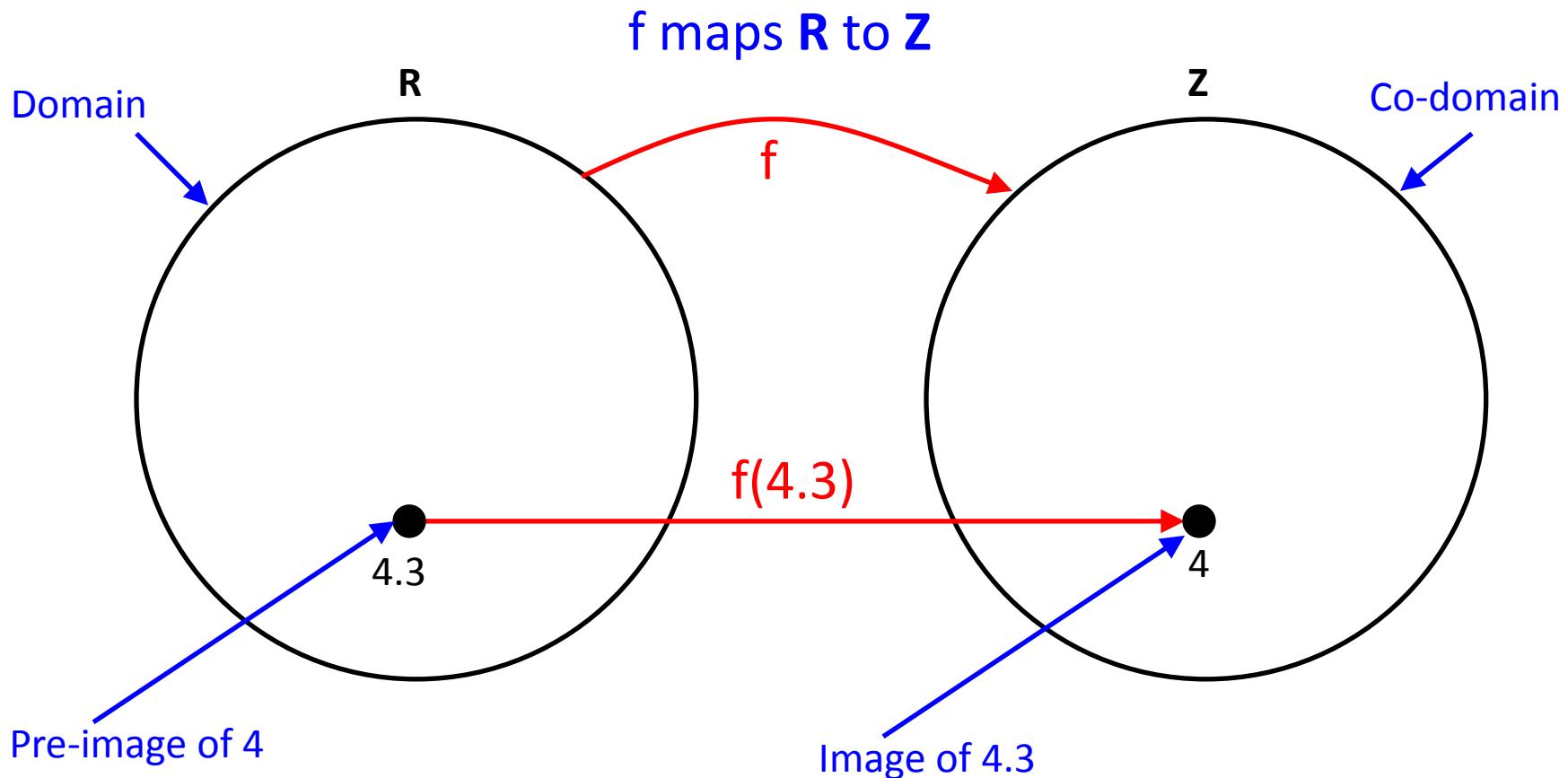
which is a total ordering. Subset $\{\dots, -5, -3, -1, 1, 3, 5, \dots\}$ of set \mathbb{Z} does not have a least element and therefore \mathbb{Z} is not a well-ordered set with respect to this relation R .

Mat2033 - Discrete Mathematics

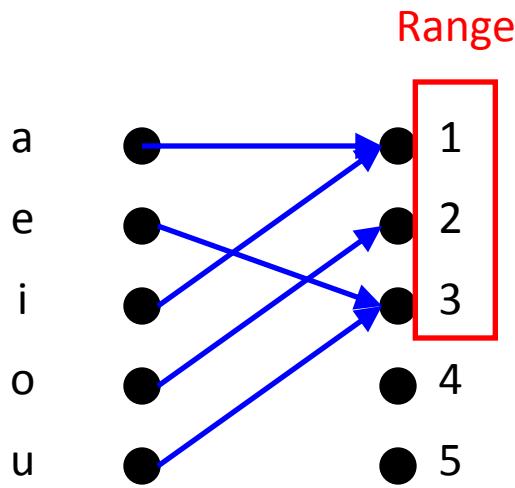
Functions

Definition of a function

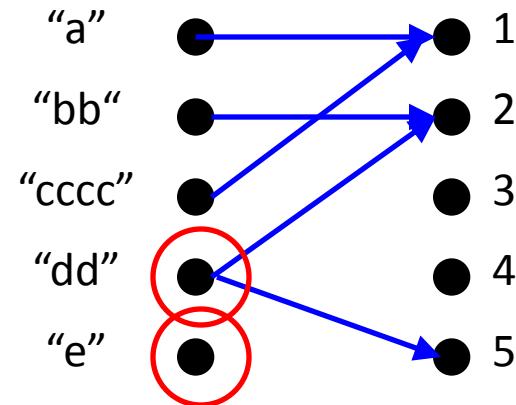
- A function takes an element from a set and maps it to a UNIQUE element in another set



Even more functions



Some function...



Not a valid function!
Also not a valid function!

Some Function Terminology

- If it is written that $f:A\rightarrow B$, and $f(a)=b$ (where $a\in A$ & $b\in B$), then we say:
 - A is the *domain* of f .
 - B is the *codomain* of f .
 - b is the *image* of a under f .
 - a is a *pre-image* of b under f .
 - In general, b may have more than 1 pre-image.
 - The *range* $R\subseteq B$ of f is $R=\{b \mid \exists a f(a)=b\}$.

We also say
the *signature*
of f is $A\rightarrow B$.

Range versus Codomain

- The range of a function might *not* be its whole codomain.
- The codomain is the set that the function is *declared* to map all domain values into.
- The range is the *particular* set of values in the codomain that the function *actually* maps elements of the domain to.

Range vs. Codomain - Example

- Suppose I declare to you that: “ f is a function mapping students in this class to the set of grades $\{A,B,C,D,E\}$.”
- At this point, you know f ’s codomain is: $\{A,B,C,D,E\}$, and its range is unknown!
- Suppose the grades turn out all As and Bs.
- Then the range of f is $\{A,B\}$, but its codomain is still $\{A,B,C,D,E\}$!.

Function arithmetic

- Let $f_1(x) = 2x$
- Let $f_2(x) = x^2$
- $f_1 + f_2 = (f_1 + f_2)(x) = f_1(x) + f_2(x) = 2x + x^2$
- $f_1 f_2 = (f_1 f_2)(x) = f_1(x) f_2(x) = 2x \cdot x^2 = 2x^3$

Example: $f_1, f_2 : \mathbb{R} \rightarrow \mathbb{R}$, $f_1(x) = x^2$, $f_2(x) = x - x^2$.

Find $f_1 + f_2$, $f_1 f_2$.

Solution: $(f_1 + f_2)(x) = f_1(x) + f_2(x) = x^2 + (x - x^2) = x$

$$(f_1 f_2)(x) = x^2(x - x^2) = x^3 - x^4$$

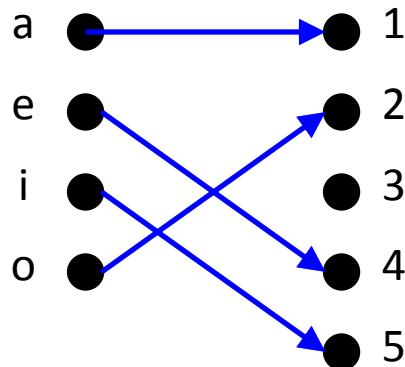
Definition: Let f be a function from the set A to the set B and let S be a subset of A . The image of S is the subset of B that consists of the images of the elements of S . We denote the image of S by $f(S)$, so that

$$f(S) = \{f(s) \mid s \in S\}$$

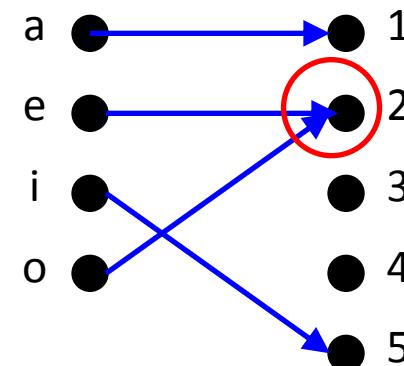
Example: Let $A = \{a, b, c, d, e\}$ and $B = \{1, 2, 3, 4\}$ with $f(a) = 2, f(b) = 1, f(c) = 4, f(d) = 1, f(e) = 1$. The image of the subset $S = \{b, c, d\}$ is the set $f(S) = \{1, 4\}$.

One-to-one functions

- A function is *one-to-one* (1-1), or *injective*, or *an injection*, iff every element of its range has *only* 1 pre-image.
 - Formally: given $f:A \rightarrow B$,
- “ x is injective” $\equiv (\neg \exists x,y: x \neq y \wedge f(x) = f(y))$.
- Only one element of the domain is mapped to any given one element of the range.
- Formal definition: A function f is one-to-one if $f(x) = f(y)$ implies $x = y$.



A one-to-one function



A function that is
not one-to-one

Example: $f: \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x)=x^2$ is NOT a one-to-one function. $f(1)=f(-1)$, but $1 \neq -1$.

Example: $f(x)=x+1$ is a one-to-one function.

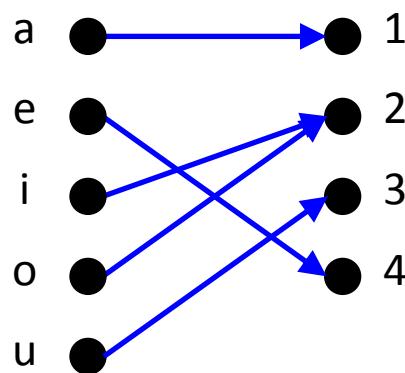
$$f(x) = f(y) (\Rightarrow x+1 = y+1 \Rightarrow x=y)$$

Definition: A function f whose domain and codomain are subsets of the set of real numbers is called strictly increasing if $f(x) < f(y)$ whenever $x < y$ and x and y are in the domain of f . Similarly, f is called strictly decreasing if $f(x) > f(y)$ whenever $x < y$ and x and y are in the domain of f .

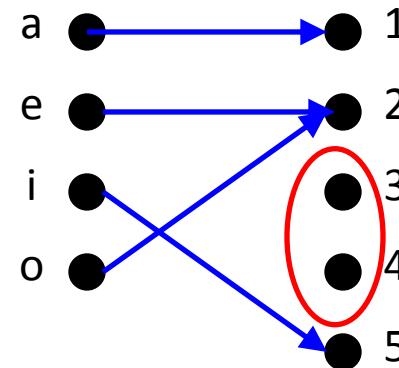
Onto functions

A function $f:A\rightarrow B$ is *onto* or *surjective* or a *surjection* iff its range is equal to its codomain
 $(\forall b \in B, \exists a \in A: f(a) = b)$.

- Formal definition: A function f is onto if for all $y \in C$, there exists $x \in D$ such that $f(x) = y$.



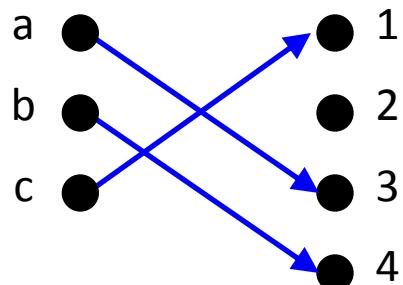
An onto function



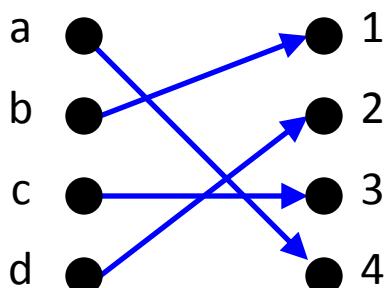
A function that is not onto

Onto vs. one-to-one

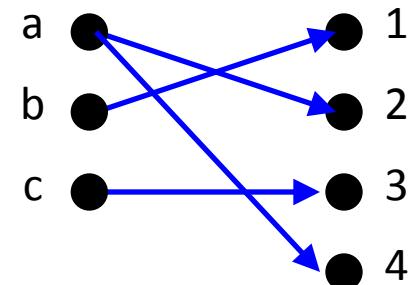
- Are the following functions onto, one-to-one, both, or neither?



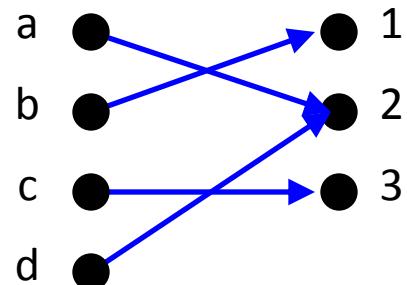
1-1, not onto



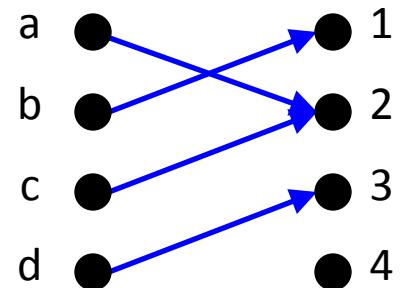
Both 1-1 and onto



Not a valid function



Onto, not 1-1



Neither 1-1 nor onto

Definition: A function from A to B is called onto, or surjective, if and only if for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$. A function f is called a surjection if it is onto.

$$\forall b \in B \exists a \in A \text{ such that } f(a) = b.$$

Example: The function $f: \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x) = x^2$ is NOT onto.
for $x = -1$ there is no element in \mathbb{Z} such that $f(x) = x^2 = -1$

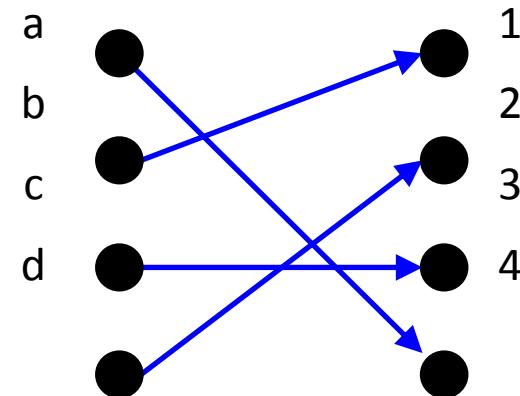
Example: $f: \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x) = x + 1$. Is f onto?

Example: $f: \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x) = x+1$. Is f onto?

Solution: For every integer y there is an integer x such that $f(x)=y$. $f(x)=y$ if and only if $x+1=y$, which holds if and only if $x=y-1$.

Bijections

- Consider a function that is both one-to-one and onto:



- Such a function is a one-to-one correspondence, or a bijection

Definition: Let A be a set. The identity function on A is the function

$$I_A : A \rightarrow A , I_A(x) = x.$$

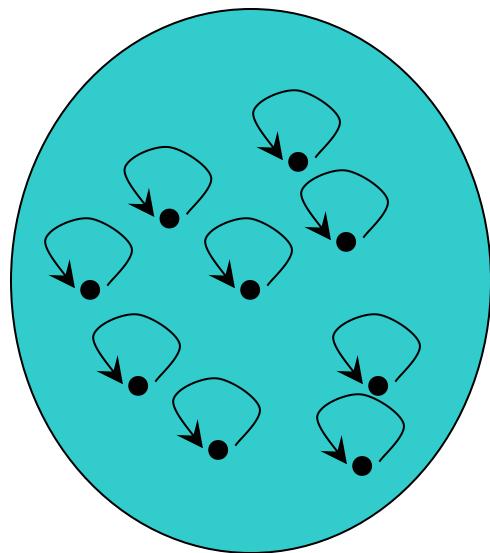
Definition: Let f be a one-to-one correspondence from the set A to the set B . The inverse function of f is the function that assigns to an element b belonging to B , the unique element a in A such that $f(a)=b$. The inverse function of f is denoted by f^{-1} . Hence, $f^{-1}(b)=a$ when $f(a)=b$.

A function f is invertible iff it is one-to-one and onto.

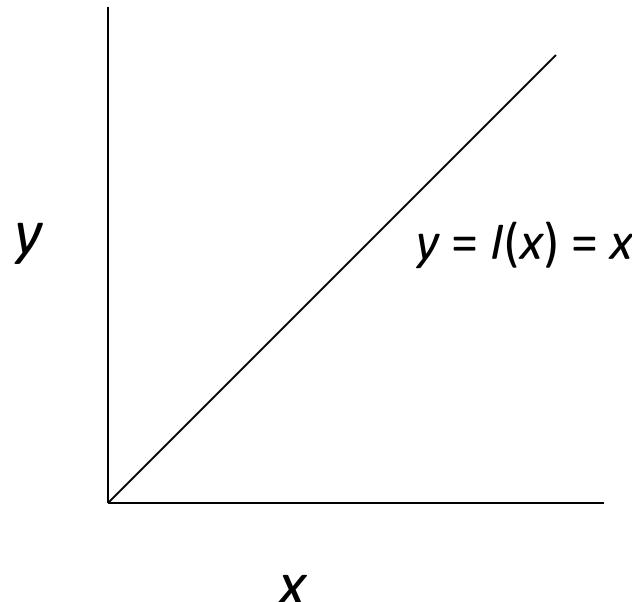
Example: $f: \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x) = x^2$ is NOT invertible because $f(-1) = f(1) = 1$. So f is not one-to-one. Hence, f is not invertible.

Identity Function Illustrations

- The identity function:

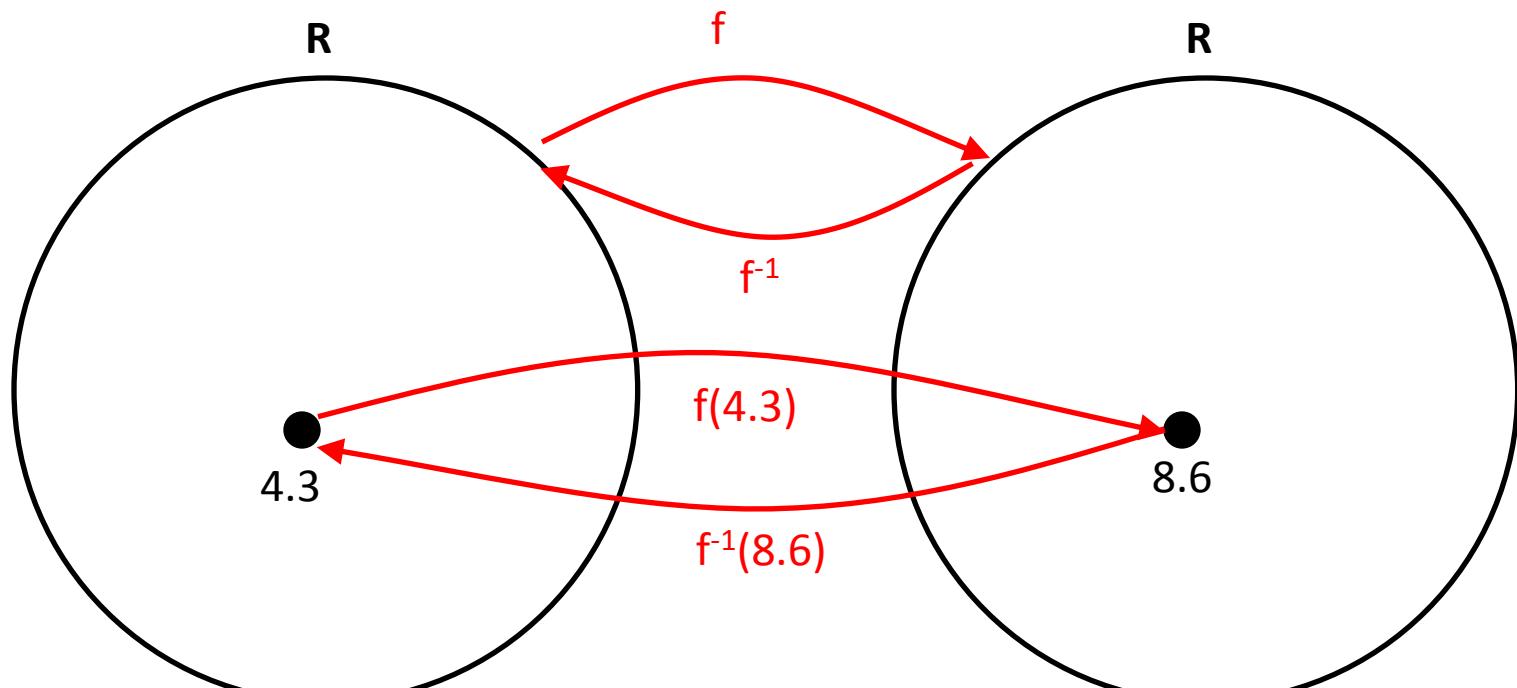


Domain and range



Inverse functions

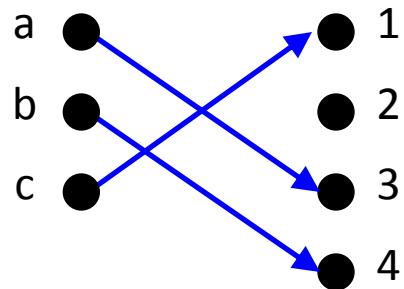
Let $f(x) = 2x$



Then $f^{-1}(x) = x/2$

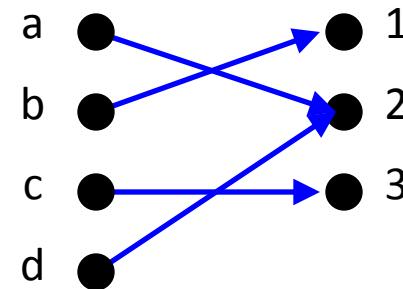
More on inverse functions

- Can we define the inverse of the following functions?



What is $f^{-1}(2)$?

Not onto!



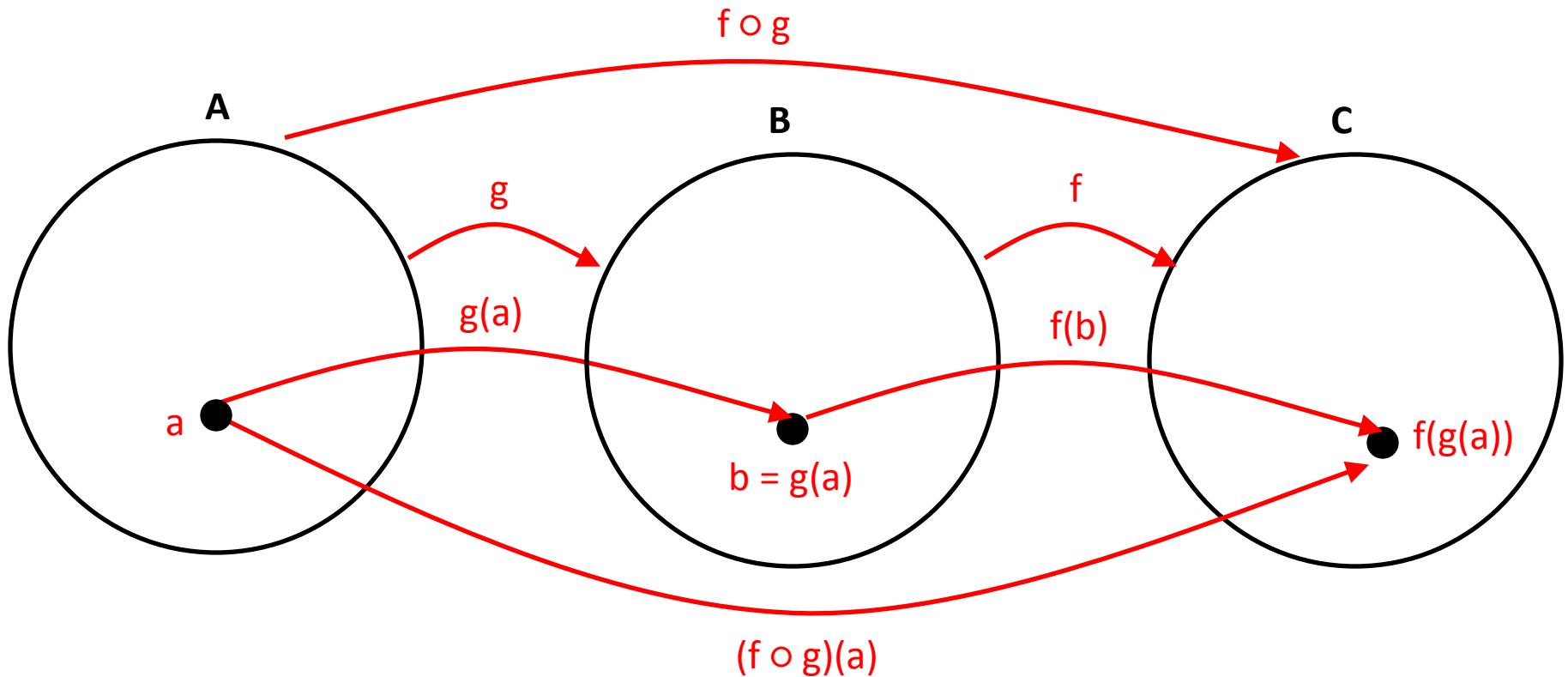
What is $f^{-1}(2)$?

Not 1-to-1!

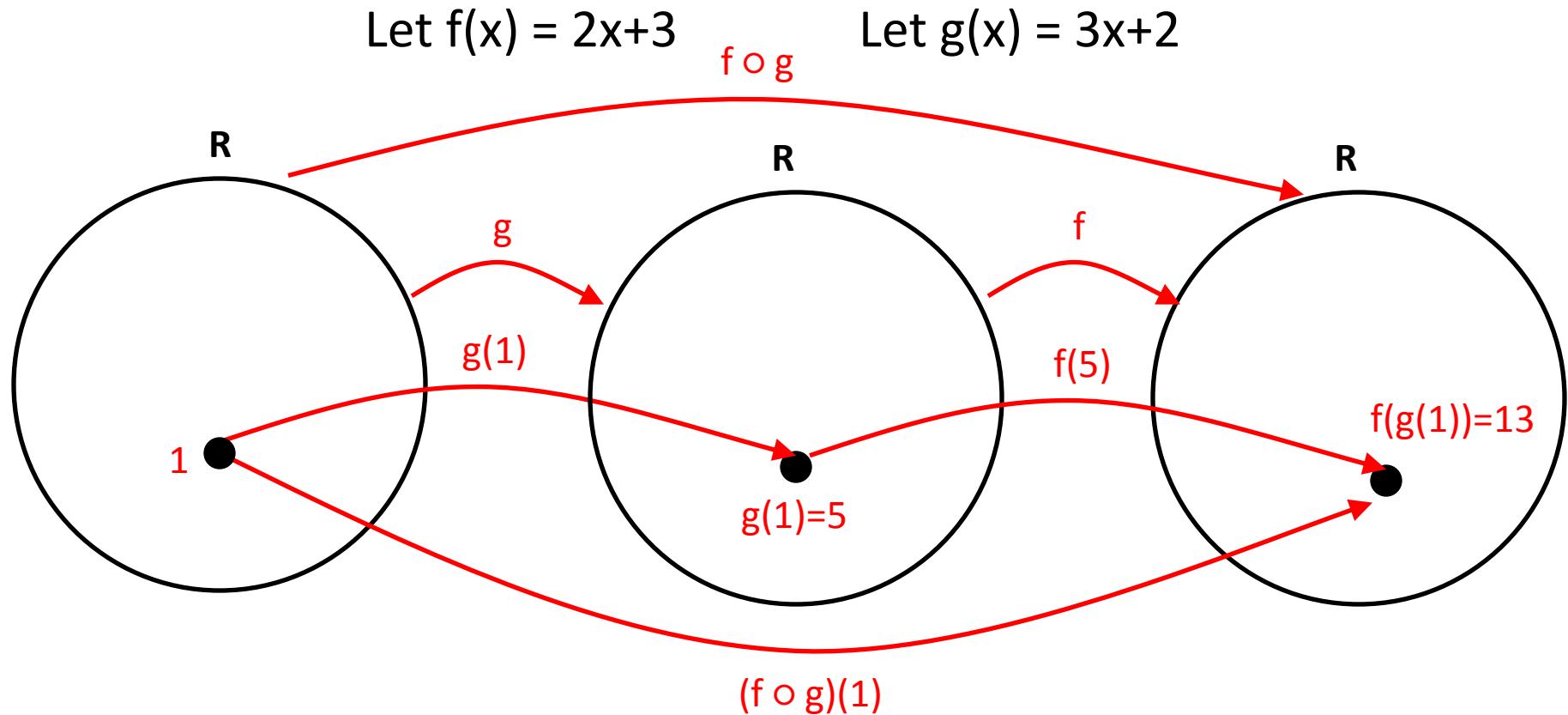
- An inverse function can ONLY be defined on a bijection

Compositions of functions

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



Compositions of functions



$$f(g(x)) = 2(3x+2)+3 = 6x+7$$

Compositions of functions

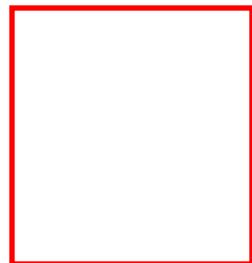
Does $f(g(x)) = g(f(x))$?

Let $f(x) = 2x+3$

Let $g(x) = 3x+2$

$$f(g(x)) = 2(3x+2)+3 = 6x+7$$

$$g(f(x)) = 3(2x+3)+2 = 6x+11$$



Not equal!

Function composition is not commutative!

Note: i) $f \circ g \neq g \circ f$. The commutative law does not hold for the composition of functions.

ii) If f is 1-1 and onto then f^{-1} exists. f composition f^{-1} gives the identity function

$$f \circ f^{-1} = f^{-1} \circ f = I$$

And

$$(f^{-1})^{-1} = f$$

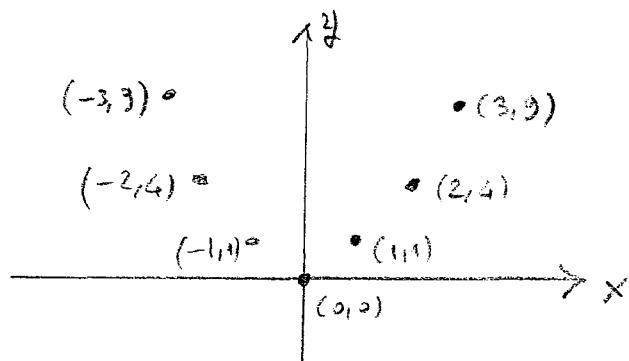
The Graphs of Functions

We can associate a set of pairs in $A \times B$ to each function from A to B. This set of pairs is called the graph of the function and is often displayed pictorially to aid in understanding the behavior of the function.

Definition: Let f be a function from the set A to the set B . The graph of the function f is the set of ordered pairs $\{(a,b) \mid a \in A \text{ and } f(a)=b\}$.

$$\text{graph } f \subseteq A \times B$$

Example: $f: \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x) = x^2$. Graph of f is



Some Important Functions

Definition: The floor function assigns to the real number x the largest integer that is less than or equal to x . The value of the floor function at x is denoted by $\lfloor x \rfloor$. The ceiling function assigns to the real number x the smallest integer that is greater than or equal to x . The value of the ceiling function at x is denoted by $\lceil x \rceil$.

Example:

$$\lfloor \frac{1}{2} \rfloor = 0, \lceil \frac{1}{2} \rceil = 1, \lfloor -\frac{1}{2} \rfloor = -1, \lceil -\frac{1}{2} \rceil = 0$$

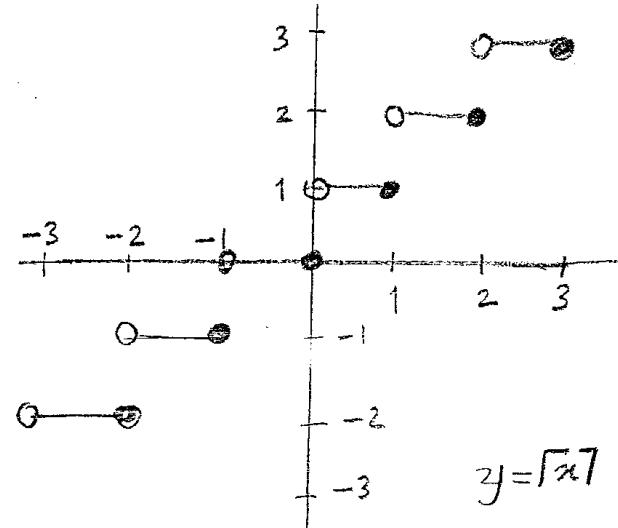
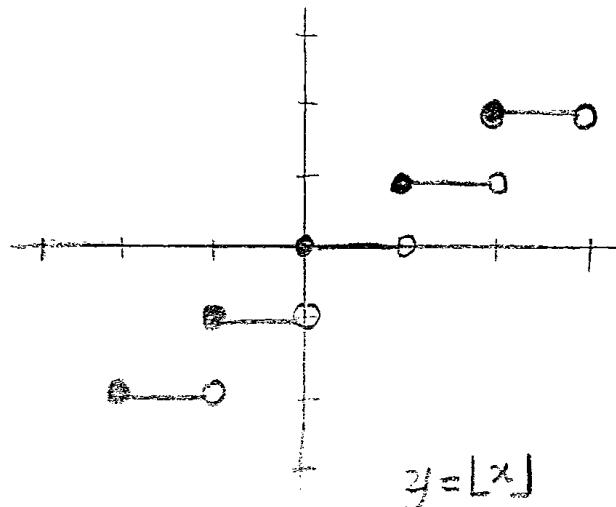
$$\lfloor 3.1 \rfloor = 3, \lceil 3.1 \rceil = 4, \lfloor 7 \rfloor = 7, \lceil 7 \rceil = 7.$$

Useful functions

- Floor: $\lfloor x \rfloor$ means take the greatest integer less than or equal to the number
- Ceiling: $\lceil x \rceil$ means take the lowest integer greater than or equal to the number

Note: The floor and ceiling functions are useful in a wide variety of applications, including those involving data storage and data transmission.

Example:



Example: Data stored on a computer disk or transmitted over a data network are usually represented as a string of bytes. Each byte is made up of 8 bits. How many bytes are required to encode 100 bits of data?

Solution:

$$\lceil \frac{100}{8} \rceil = \lceil 12.5 \rceil = 13 \text{ bytes is required.}$$

Ceiling and floor properties

Let n be an integer

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

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

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

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

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

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

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

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

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

Ceiling property proof

- Prove rule 4a: $\lfloor x+n \rfloor = \lfloor x \rfloor + n$
 - Where n is an integer
 - Will use rule 1a: $\lfloor x \rfloor = n$ if and only if $n \leq x < n+1$
- Direct proof!
 - Let $m = \lfloor x \rfloor$
 - Thus, $m \leq x < m+1$ (by rule 1a)
 - Add n to both sides: $m+n \leq x+n < m+n+1$
 - By rule 1a, $m+n = \lfloor x+n \rfloor$
 - Since $m = \lfloor x \rfloor$, $m+n$ also equals $\lfloor x \rfloor + n$
 - Thus, $\lfloor x \rfloor + n = m+n = \lfloor x+n \rfloor$

Factorial

- Factorial is denoted by $n!$
- $n! = n \cdot (n-1) \cdot (n-2) \dots 2 \cdot 1$
- Thus, $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$
- Note that $0!$ is defined to equal 1

Proving Function problems

- Let f be an invertible function from Y to Z
- Let g be an invertible function from X to Y
- Show that the inverse of $f \circ g$ is:
 - $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$

(Pf) Thus, we want to show, for all $x \in X$

$$((f \circ g) \circ (g^{-1} \circ f^{-1})) (x) = x \text{ and } ((g^{-1} \circ f^{-1}) \circ (f \circ g)) (x) = x$$

$$\begin{aligned} ((f \circ g) \circ (g^{-1} \circ f^{-1})) (x) &= (f \circ g) ((g^{-1} \circ f^{-1})) (x) \\ &= (f \circ g) (g^{-1} (f^{-1}(x))) \\ &= (f (g (g^{-1} (f^{-1}(x)))))) \\ &= (f (f^{-1}(x))) \\ &= x \end{aligned}$$

The second equality is similar

In the questions below determine whether the rule describes a function with the given domain and codomain.

$f: \mathbb{N} \rightarrow \mathbb{N}$ where $f(n) = \sqrt{n}$.

$f: \mathbb{N} \rightarrow \mathbb{N}$ where $f(n) = \sqrt{n}$.

Ans: Not a function; $f(2)$ is not an integer.

$f : \mathbb{N} \rightarrow \mathbb{N}$ where $f(n) = \sqrt{n}$.

Ans: Not a function; $f(2)$ is not an integer.

$h : \mathbb{R}^+ \rightarrow \mathbb{R}$ where $h(x) = \sqrt{x}$.

$f : \mathbb{N} \rightarrow \mathbb{N}$ where $f(n) = \sqrt{n}$.

Ans: Not a function; $f(2)$ is not an integer.

$h : \mathbb{R}^+ \rightarrow \mathbb{R}$ where $h(x) = \sqrt{x}$.

Ans: Function.

$F : \mathbf{R} \rightarrow \mathbf{R}$ where $F(x) = \frac{1}{x-5}$.

$$F : \mathbf{R} \rightarrow \mathbf{R} \text{ where } F(x) = \frac{1}{x-5}$$

Ans: Not a function; $F(5)$ not defined.

$$F : \mathbf{R} \rightarrow \mathbf{R} \text{ where } F(x) = \frac{1}{x-5} .$$

Ans: Not a function; $F(5)$ not defined.

$$F : \mathbf{Z} \rightarrow \mathbf{R} \text{ where } F(x) = \frac{1}{x^2 - 5} .$$

$$F : \mathbf{R} \rightarrow \mathbf{R} \text{ where } F(x) = \frac{1}{x-5} .$$

Ans: Not a function; $F(5)$ not defined.

$$F : \mathbf{Z} \rightarrow \mathbf{R} \text{ where } F(x) = \frac{1}{x^2 - 5} .$$

Ans: Function.

$$F : \mathbf{R} \rightarrow \mathbf{R} \text{ where } F(x) = \frac{1}{x-5} .$$

Ans: Not a function; $F(5)$ not defined.

$$F : \mathbf{Z} \rightarrow \mathbf{R} \text{ where } F(x) = \frac{1}{x^2 - 5} .$$

Ans: Function.

$$F : \mathbf{Z} \rightarrow \mathbf{Z} \text{ where } F(x) = \frac{1}{x^2 - 5} .$$

$$F : \mathbb{R} \rightarrow \mathbb{R} \text{ where } F(x) = \frac{1}{x-5} .$$

Ans: Not a function; $F(5)$ not defined.

$$F : \mathbb{Z} \rightarrow \mathbb{R} \text{ where } F(x) = \frac{1}{x^2 - 5} .$$

Ans: Function.

$$F : \mathbb{Z} \rightarrow \mathbb{Z} \text{ where } F(x) = \frac{1}{x^2 - 5} .$$

Ans: Not a function; $F(1)$ not an integer.

$\therefore G : \mathbf{R} \rightarrow \mathbf{R}$ where $G(x) = \begin{cases} x+2 & \text{if } x \geq 0 \\ x-1 & \text{if } x \leq 4 \end{cases}$

$\therefore G : \mathbf{R} \rightarrow \mathbf{R}$ where $G(x) = \begin{cases} x+2 & \text{if } x \geq 0 \\ x-1 & \text{if } x \leq 4 \end{cases}$

Ans: Not a function; the cases overlap. For example, $G(1)$

i. $f: \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = \begin{cases} x^2 & \text{if } x \leq 2 \\ x-1 & \text{if } x \geq 4 \end{cases}$

$f: \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = \begin{cases} x^2 & \text{if } x \leq 2 \\ x-1 & \text{if } x \geq 4 \end{cases}$

Ans: Not a function; $f(3)$ not defined.

i. $G : \mathbb{Q} \rightarrow \mathbb{Q}$ where $G(p/q) = q$.

i. $G : \mathbb{Q} \rightarrow \mathbb{Q}$ where $G(p/q) = q$.

Ans: Not a function; $f(1/2) = 2$ and $f(2/4) = 4$.

Give an example of a function $f: \mathbf{Z} \rightarrow \mathbf{Z}$ that is 1-1 and not onto \mathbf{Z} .

Give an example of a function $f: \mathbb{Z} \rightarrow \mathbb{Z}$ that is 1-1 and not onto \mathbb{Z} .
Ans: $f(n) = 2n$.

Give an example of a function $f: \mathbb{Z} \rightarrow \mathbb{Z}$ that is 1-1 and not onto \mathbb{Z} .
Ans: $f(n) = 2n$.

Give an example of a function $f: \mathbb{Z} \rightarrow \mathbb{Z}$ that is onto \mathbb{Z} but not 1-1.

Give an example of a function $f: \mathbb{Z} \rightarrow \mathbb{Z}$ that is 1-1 and not onto \mathbb{Z} .

Ans: $f(n) = 2n$.

Give an example of a function $f: \mathbb{Z} \rightarrow \mathbb{Z}$ that is onto \mathbb{Z} but not 1-1.

Ans: $f(n) = \left\lfloor \frac{n}{2} \right\rfloor$.

Give an example of a function $f: \mathbf{Z} \rightarrow \mathbf{Z}$ that is 1-1 and not onto \mathbf{Z} .

Ans: $f(n) = 2n$.

Give an example of a function $f: \mathbf{Z} \rightarrow \mathbf{Z}$ that is onto \mathbf{Z} but not 1-1.

Ans: $f(n) = \left\lfloor \frac{n}{2} \right\rfloor$.

Give an example of a function $f: \mathbf{Z} \rightarrow \mathbf{N}$ that is both 1-1 and onto \mathbf{N} .

Give an example of a function $f: \mathbf{Z} \rightarrow \mathbf{Z}$ that is 1-1 and not onto \mathbf{Z} .

Ans: $f(n) = 2n$.

Give an example of a function $f: \mathbf{Z} \rightarrow \mathbf{Z}$ that is onto \mathbf{Z} but not 1-1.

Ans: $f(n) = \left\lfloor \frac{n}{2} \right\rfloor$.

Give an example of a function $f: \mathbf{Z} \rightarrow \mathbf{N}$ that is both 1-1 and onto \mathbf{N} .

Ans: $f(n) = \begin{cases} -2n & \text{if } n \leq 0 \\ 2n-1 & \text{if } n > 0 \end{cases}$

Suppose $f: \mathbf{N} \rightarrow \mathbf{N}$ has the rule $f(n) = 4n + 1$. Determine whether f is 1-1.

Ans:

Suppose $f: \mathbf{N} \rightarrow \mathbf{N}$ has the rule $f(n) = 4n + 1$. Determine whether f is onto \mathbf{N} .

Ans:

Suppose $f: \mathbf{Z} \rightarrow \mathbf{Z}$ has the rule $f(n) = 3n^2 - 1$. Determine whether f is 1-1.

Ans:

Suppose $f: \mathbf{Z} \rightarrow \mathbf{Z}$ has the rule $f(n) = 3n - 1$. Determine whether f is onto \mathbf{Z} .

Ans:

Suppose $f: \mathbf{N} \rightarrow \mathbf{N}$ has the rule $f(n) = 3n^2 - 1$. Determine whether f is 1-1.

Ans:

Suppose $f: \mathbf{N} \rightarrow \mathbf{N}$ has the rule $f(n) = 4n^2 + 1$. Determine whether f is onto \mathbf{N}

Ans:

Suppose $f: \mathbf{N} \rightarrow \mathbf{N}$ has the rule $f(n) = 4n + 1$. Determine whether f is 1-1.

Ans: Yes.

Suppose $f: \mathbf{N} \rightarrow \mathbf{N}$ has the rule $f(n) = 4n + 1$. Determine whether f is onto \mathbf{N} .

Ans: No.

Suppose $f: \mathbf{Z} \rightarrow \mathbf{Z}$ has the rule $f(n) = 3n^2 - 1$. Determine whether f is 1-1.

Ans: No.

Suppose $f: \mathbf{Z} \rightarrow \mathbf{Z}$ has the rule $f(n) = 3n - 1$. Determine whether f is onto \mathbf{Z} .

Ans: No.

Suppose $f: \mathbf{N} \rightarrow \mathbf{N}$ has the rule $f(n) = 3n^2 - 1$. Determine whether f is 1-1.

Ans: Yes.

Suppose $f: \mathbf{N} \rightarrow \mathbf{N}$ has the rule $f(n) = 4n^2 + 1$. Determine whether f is onto \mathbf{N}

Ans: No.

$$f(n) = \begin{cases} \frac{-n}{2}, & n \text{ even} \\ \frac{n^2 + 1}{2}, & n \text{ odd} \end{cases}$$

is $f: \mathbb{N} \rightarrow \mathbb{Z}$ 1-1 and onto \mathbb{Z} ?

$$f(n) = \begin{cases} -2n, & n \leq 0 \\ 2n+1, & n > 0 \end{cases}$$

an example of a function $f: \mathbf{Z} \rightarrow \mathbf{N}$ that is 1-1 and not onto \mathbf{N} .

$$f(n) = \begin{cases} \frac{-n}{2}, & n \text{ even.} \\ \frac{n-1}{2}, & n \text{ odd} \end{cases}$$

an example of a function $f: \mathbb{N} \rightarrow \mathbb{Z}$ that is onto \mathbb{Z} and not 1-1.

Let $f(x) = \lfloor x^3/3 \rfloor$. Find $f(S)$ if S is:

- (a) $\{-2, -1, 0, 1, 2, 3\}$.
- (b) $\{0, 1, 2, 3, 4, 5\}$.
- (c) $\{1, 5, 7, 11\}$.
- (d) $\{2, 6, 10, 14\}$.

Ans: (a) $\{-3, -1, 0, 2, 9\}$.

- (b) $\{0, 2, 9, 21, 41\}$.
- (c) $\{0, 41, 114, 443\}$.
- (d) $\{2, 72, 333, 914\}$.

Mat2033 - Discrete Mathematics

Integers and division

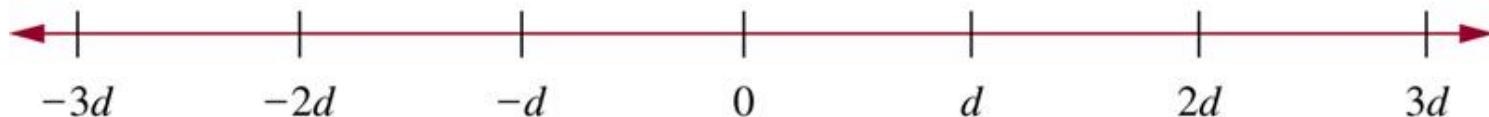
Integers and division

- **Number theory:** the branch of mathematics involves integers and their properties.
- If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$.
- When a divides b we say that a is a factor of b and that b is a multiple of a .
- The notation $a|b$ denotes a divides b . We write $a \nmid b$ when a does not divide b .

Example: Let n and d be positive integers. How many positive integers not exceeding n are divisible by d ?

- The positive integers divisible by d are all integers of them form dk , where k is a positive integer
- Thus, there are $\lfloor n/d \rfloor$ positive integers not exceeding n that are divisible by d

© The McGraw-Hill Companies, Inc. all rights reserved.



Theorem 1: Let a , b , and c be integers, then

1. If $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
2. If $a \mid b$ then $a \mid bc$ for all integers c
3. If $a \mid b$ and $b \mid c$, then $a \mid c$

Proof:

1. From the definition of divisibility there are integers s and t with $b=as$ and $c=at$. Hence,

$$b+c = as+at = a(s+t).$$

Therefore a divides $b+c$.

2. If $a \mid b$ then $b=as$ for some $s \in \mathbb{Z}$. Multiply b with c then we get $bc = asc = a(sc)$. Since $sc \in \mathbb{Z}$ then from the definition of divisibility $a \mid bc$.

3. If $a \mid b$ then $b=as$ for some $s \in \mathbb{Z}$. Similarly, $c=bt$ for some $t \in \mathbb{Z}$. If we write as instead of b in the second equation we get $c=ast$. Since $st \in \mathbb{Z}$, this means $a \mid c$.

Corollary-1: If a , b and c are integers such that
 $a \mid b$ and $a \mid c$, then $a \mid mb+nc$ whenever m and n are
integers.

Corollary-1: If a, b and c are integers such that $a|b$ and $a|c$, then $a|m(b+nc)$ whenever m and n are integers.

Proof: By part(2) of thm-1 it follows that $a|m(b+nc)$ whenever m and n are integers. By part(1) of thm-1 it follows that $a|m(b+nc)$.

The division algorithm

- Let a be integer and d be a positive integer. Then there are unique integers q and r with $0 \leq r < d$, such that $a=dq+r$.
- In the equality, d is the divisor, a is the dividend, q is the quotient, r is the remainder

$$q = a \text{ div } d, \quad r = a \text{ mod } d$$

- -11 divided by 3
- $-11=3(-4)+1$, $-4=-11 \text{ div } 3$, $1=-11 \text{ mod } 3$
- $-11=3(-3)-2$, but remainder cannot be negative

Example: What are the quotient and remainder when 701
is divided by 11?

Example: What are the quotient and remainder when 101 is divided by 11?

Solution: $101 = 11 \cdot 9 + 2$. The quotient when 101 is divided by 11 is $q = 101 \text{ div } 11$, and the remainder is $r = 101 \text{ mod } 11$

Example: What are the quotient and remainder when 101 is divided by 11?

Solution: $101 = 11 \cdot 9 + 2$. The quotient when 101 is divided by 11 is $q = 101 \text{ div } 11$, and the remainder is $r = 101 \text{ mod } 11$.

Example: What are the quotient and remainder when -11 is divided by 3?

Example: What are the quotient and remainder when 101 is divided by 11?

Solution: $101 = 11 \cdot 9 + 2$. The quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$, and the remainder is $2 = 101 \bmod 11$.

Example: What are the quotient and remainder when -11 is divided by 3?

Solution: $-11 = 3(-4) + 1$. The quotient is $-4 = -11 \text{ div } 3$, and the remainder is $1 = -11 \bmod 3$.

Example: What are the quotient and remainder when 101 is divided by 11?

Solution: $101 = 11 \cdot 9 + 2$. The quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$, and the remainder is $2 = 101 \bmod 11$.

Example: What are the quotient and remainder when -11 is divided by 3?

Solution: $-11 = 3(-4) + 1$. The quotient is $-4 = -11 \text{ div } 3$, and the remainder is $1 = -11 \bmod 3$.

Note: The remainder cannot be negative. So we cannot write in the above example

$$-11 = 3(-3) - 2$$

Since $r = -2$ does not satisfy $0 \leq r < 3$.

Example: What are the quotient and remainder when 101 is divided by 11?

Solution: $101 = 11 \cdot 9 + 2$. The quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$, and the remainder is $2 = 101 \bmod 11$.

Example: What are the quotient and remainder when -11 is divided by 3?

Solution: $-11 = 3(-4) + 1$. The quotient is $-4 = -11 \text{ div } 3$, and the remainder is $1 = -11 \bmod 3$.

Note: The remainder cannot be negative. So we cannot write in the above example

$$-11 = 3(-3) - 2$$

Since $r = -2$ does not satisfy $0 \leq r < 3$.

Note: a is divisible by d if and only if the remainder is zero.

Primes and greatest common divisions

- **Prime:** a positive integer p greater than 1 if the only positive factors of p are 1 and p
- A positive integer greater than 1 that is not prime is called **composite**

Remark: The integer n is composite if and only if there exists an integer a such that $a|n$ and $1 < a < n$.

The primes less than 100 are:

2	3	5	7	11	13	17	19	23
29	31	37	41	43	47	53	59	61
67	71	73	79	83	89	97		

Theorem:(Fundamental theorem of arithmetic) Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes when the prime factors are written in order of non-decreasing size

Example: Prime factorizations of integers

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$$

$$641 = 641$$

$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$$

$$1024 = 2 \cdot 2 = 2^{10}$$

Note: Let $m \in \mathbb{N}$ be a positive integer and p_1, p_2, \dots, p_n be distinct primes and $\alpha_1, \alpha_2, \dots, \alpha_n$ be nonnegative integers then m can be written as

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

Theorem: If n is a composite integer, then n has a prime division less than or equal to \sqrt{n} .

- As n is composite, n has a factor $1 < a < n$, and thus $n = ab$.
- We show that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ (by contraposition)
- Thus n has a divisor not exceeding \sqrt{n} .
- This divisor is either prime or by the fundamental theorem of arithmetic, has a prime divisor less than itself, and thus a prime divisor less than \sqrt{n} .

Note: An integer is prime if it is not divisible by any prime less than or equal to its square root.

Example: Show that 101 is prime

- The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, 7
- As 101 is not divisible by 2, 3, 5, 7, it follows that 101 is prime

Procedure for prime factorization

- Begin by diving n by successive primes, starting with 2.
- If n has a prime factor, we would find a prime factor not exceeding \sqrt{n} .
- If no prime factor is found, then n is prime.
- Otherwise, if a prime factor p is found, continue by factoring n/p .
- Note that n/p has no prime factors less than p .
- If n/p has no prime factor greater than or equal to p and not exceeding its square root, then it is prime.
- Otherwise, continue by factoring $n/(pq)$.
- Continue until factorization has been reduced to a prime.

Example: Find the prime factorization of 7007.

- Start with 2, 3, 5, and then 7, $7007/7=1001$
- Then, divide 1001 by successive primes, beginning with 7, and find $1001/7=143$
- Continue by dividing 143 by successive primes, starting with 7, and find $143/11=13$
- As 13 is prime, the procedure stops
- $7007=7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$

Theorem

Theorem: There are infinitely many primes.

- Proof by contradiction.
- Assume that there are only finitely many primes, p_1, p_2, \dots, p_n . Let $Q = p_1 p_2 \dots p_n + 1$
- By Fundamental Theorem of Arithmetic: Q is prime or else it can be written as the product of two or more primes.

Theorem

- However, none of the primes p_j divides Q , for if $p_j \mid Q$, then p_j divides $Q - p_1 p_2 \dots p_n = 1$
- Hence, there is a prime not in the list p_1, p_2, \dots, p_n
- This prime is either Q , if it is prime, or a prime factor for Q
- This is a contradiction as we assumed that we have listed all the primes

Greatest common divisors

- Let a and b be integers, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the **greatest common divisor** (GCD) of a and b , often denoted as $\gcd(a,b)$

Greatest common divisors

- The integers a and b are **relative prime** if their GCD is 1

$$\gcd(10, 17)=1,$$

$$\gcd(10, 21)=1,$$

$$\gcd(10, 24)=2$$

- The integers a_1, a_2, \dots, a_n are **pairwise relatively prime** if $\gcd(a_i, a_j)=1$ whenever $1 \leq i < j \leq n$

Example: What is the common divisor of 24 and 36?

Example: What is the common divisor of 24 and 36?

Solution: The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6 and 12. Hence $\gcd(24, 36) = 12$.

Example: What is the common divisor of 24 and 36?

Solution: The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6 and 12. Hence $\text{gcd}(24, 36) = 12$.

Definition-5: The integers a and b are relatively prime if their greatest common divisor is 1.

Example: What is the common divisor of 24 and 36?

Solution: The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6 and 12. Hence $\text{gcd}(24, 36) = 12$.

Definition-5: The integers a and b are relatively prime if their greatest common divisor is 1.

Example: The positive common divisor of 17 and 22 is 1 so 17 and 22 are relatively prime. So $\text{gcd}(17, 22) = 1$

Example: What is the common divisor of 24 and 36?

Solution: The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6 and 12. Hence $\gcd(24, 36) = 12$.

Definition-5: The integers a and b are relatively prime if their greatest common divisor is 1.

Example: The positive common divisor of 17 and 22 is 1 so 17 and 22 are relatively prime. So $\gcd(17, 22) = 1$

Definition-6: The integers a_1, a_2, \dots, a_n are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Prime factorization and GCD

- Finding GCD

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$$

$$120 = 2^3 \cdot 3 \cdot 5, \quad 500 = 2^2 \cdot 5^3$$

$$\gcd(120, 500) = 2^2 \cdot 3^0 \cdot 5^1 = 20$$

Least common multiple

- **Least common multiples** of the positive integers a and b is the smallest positive integer that is divisible by both a and b , denoted as $\text{lcm}(a,b)$

Least common multiple

- Finding LCM

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

$$\text{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$$

$$120 = 2^3 \cdot 3 \cdot 5, 500 = 2^2 \cdot 5^3$$

$$\text{lcm}(120, 500) = 2^3 \cdot 3^1 \cdot 5^3 = 8 \cdot 3 \cdot 125 = 3000$$

Theorem: Let a and b be positive integers, then

$$ab = \gcd(a,b) \cdot \text{lcm}(a,b)$$

Modular arithmetic

- If a and b are integers and m is a positive integer, then a is **congruent** to b modulo m if m divides $a-b$
- We use the notation $a \equiv b \pmod{m}$ to indicate that a is **congruent** to b modulo m . If a and b are not congruent modulo m , we write $a \not\equiv b \pmod{m}$
- Let a and b be integers, m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$

Example: Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are not congruent modulo 6

$$17-5=12, \text{ we see } 17 \equiv 5 \pmod{6}$$

$$24-14=10, \text{ and thus } 24 \not\equiv 14 \pmod{6}$$

Theorem: Let m be a positive integer. The integer a and b are congruent modulo m if and only if there is an integer k such that $a=b+km$.

(\Rightarrow) If $a=b+km$, then $km=a-b$, and thus m divides $a-b$ and so $a \equiv b \pmod{m}$

(\Leftarrow) if $a \equiv b \pmod{m}$, then $m|a-b$. Thus, $a-b=km$, and so $a=b+km$

Theorem: Let m be a positive integer.

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a+c \equiv b+d \pmod{m} \text{ and } ac \equiv bd \pmod{m}.$$

Proof:

Since $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, there are integers t and s such that $b = a + sm$ and $d = c + tm$. Therefore

$$b+d = (a+c) + m(s+t),$$

$$bd = (a+sm)(c+tm) = ac + m(at+cs+stm)$$

Hence $a+c \equiv b+d \pmod{m}$, and $ac \equiv bd \pmod{m}$

Example: $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, so

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$$

$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}$$

Corollary: Let a and b be integers and m be a positive integer, then

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

Proof: By definitions mod m and congruence modulo m , we know that $a \equiv (a \bmod m) \pmod{m}$ and $b \equiv (b \bmod m) \pmod{m}$. Hence

$$(a+b) \equiv ((a \bmod m) + (b \bmod m)) \pmod{m}$$

$$ab \equiv (a \bmod m)(b \bmod m) \pmod{m}$$

Theorem - 9: Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof: If $a \equiv b \pmod{m}$, then $m | (a-b)$. This means that there is an integer k such that $a-b=km$, so that $a=b+km$. Conversely, if there is an integer k such that $a=b+km$, then $km=a-b$. Hence m divides $a-b$, so that $a \equiv b \pmod{m}$.

Note: The set of all integers congruent to an integer a modulo m is called the congruence class of a modulo m .

Applications of Congruences

Cryptology:

Congruences have many applications to discrete mathematics and computer science. One of the most important applications of congruences involves cryptology, which is the study of secret messages. One of the earliest known uses of cryptology was by Julius Caesar. He made messages secret by shifting each letter three letters forward in the alphabet (sending the last three letters of the alphabet to the first three). For instance, using this scheme the letter B is sent to E and the letter X is sent to A. This is an example of encryption, that is, the process of making a message secret.

To express Caesar's encryption process mathematically, first replace each letter by an integer from 0 to 25, based on its position in the alphabet. For example, replace A by 0, K by 10, and Z by 25. Caesar's encryption method can be represented by the function f that assigns to the nonnegative integer p , $p \leq 25$, the integer $f(p)$ in the set $\{0, 1, 2, \dots, 25\}$ with

$$f(p) = (p+3) \bmod 26$$

In the encrypted version of the message, the letter represented by p is replaced with the letter represented by $(p+3) \bmod 26$.

Example: What is the secret message produced from the message "MEET YOU IN THE PARK" using the Caesar's cipher?

Solution: First replace the letters in the message with numbers. This produces

12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10.

Now replace each of these numbers p by $f(p) = (p+3) \bmod 26$.
This gives

15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13 .

Translating this back to letters produces the encrypted message "PHHW BRX LQ WKH SDUN".

To recover the original message from a secret message encrypted by the Caesar's cipher, the function f^{-1} , the inverse of f , is used. f^{-1} sends an integer p from $\{0, 1, 2, \dots, 25\}$ to $f^{-1}(p) = (p - 3) \bmod 26$. In other words, to find the original message, each letter is shifted back three letters in the alphabet, with the first three letters sent to the last three letters of the alphabet. The process of determining the original message from the encrypted message is called decryption.

It is possible to generalize Caesar's method. For example we can shift any letter by k , so that

$$f(p) = (p + k) \bmod 26.$$

Such a cipher is called a shift cipher. Note that decryption can be carried out using

$$f^{-1}(P) = (P - k) \bmod 26.$$

Obviously, Caesar's method and shift ciphers do not provide a high level of security. There are various ways to enhance this method. One approach that slightly enhances the security is to use a function of the form

$$f(P) = (ap + b) \bmod 26$$

where a and b are integers, chosen such that f is a bijection (1-1 and onto). Such a mapping is called an affine transformation.

Example: What letter replaces the letter K when the function $f(p) = (7p+3) \bmod 26$ is used for encryption?

Example: What letter replaces the letter K when the function $f(p) = (7p+3) \bmod 26$ is used for encryption?

Solution: 10 represents K, then $f(10) = (7 \cdot 10 + 3) \bmod 26 = 21$.
21 represents V. K is replaced by V in the encrypted message.

EXAMPLE

Encrypt the plaintext message “STOP GLOBAL WARMING” using the shift cipher with shift $k = 11$.

Solution: To encrypt the message “STOP GLOBAL WARMING” we first translate each letter to the corresponding element of \mathbf{Z}_{26} . This produces the string

18 19 14 15 6 11 14 1 0 11 22 0 17 12 8 13 6.

We now apply the shift $f(p) = (p + 11) \bmod 26$ to each number in this string. We obtain

3 4 25 0 17 22 25 12 11 22 7 11 2 23 19 24 17.

Translating this last string back to letters, we obtain the ciphertext “DEZA RWZMLW HLCX-TYR.” 

EXAMPLE

Decrypt the ciphertext message “LEWLYPLUJL PZ H NYLHA ALHJOLY” that was encrypted with the shift cipher with shift $k = 7$.

Solution: To decrypt the ciphertext “LEWLYPLUJL PZ H NYLHA ALHJOLY” we first translate the letters back to elements of \mathbf{Z}_{26} . We obtain

$$11 \ 4 \ 22 \ 11 \ 24 \ 15 \ 11 \ 20 \ 9 \ 11 \quad 15 \ 25 \quad 7 \quad 13 \ 24 \ 11 \ 7 \ 0 \quad 0 \ 11 \ 7 \ 9 \ 14 \ 11 \ 24.$$

Next, we shift each of these numbers by $-k = -7$ modulo 26 to obtain

$$4 \ 23 \ 15 \ 4 \ 17 \ 8 \ 4 \ 13 \ 2 \ 4 \quad 8 \ 18 \quad 0 \quad 6 \ 17 \ 4 \ 0 \ 19 \quad 19 \ 4 \ 0 \ 2 \ 7 \ 4 \ 17.$$

Finally, we translate these numbers back to letters to obtain the plaintext. We obtain “EXPERIENCE IS A GREAT TEACHER.” 

Exercises

1. Encrypt the message DO NOT PASS GO by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.
 - a) $f(p) = (p + 3) \text{ mod } 26$ (the Caesar cipher)
 - b) $f(p) = (p + 13) \text{ mod } 26$
 - c) $f(p) = (3p + 7) \text{ mod } 26$

2. Encrypt the message STOP POLLUTION by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.
- a) $f(p) = (p + 4) \text{ mod } 26$
 - b) $f(p) = (p + 21) \text{ mod } 26$
 - c) $f(p) = (17p + 22) \text{ mod } 26$

3. Encrypt the message WATCH YOUR STEP by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.
- a) $f(p) = (p + 14) \text{ mod } 26$
 - b) $f(p) = (14p + 21) \text{ mod } 26$
 - c) $f(p) = (-7p + 1) \text{ mod } 26$

4. Decrypt these messages that were encrypted using the Caesar cipher.
- a) EOXH MHDQV
 - b) WHVW WRGDB
 - c) HDW GLP VXP
5. Decrypt these messages encrypted using the shift cipher $f(p) = (p + 10) \text{ mod } 26$.
- a) CEBBOXNOB XYG
 - b) LO WI PBSOXN
 - c) DSWO PYB PEX

- What is the decryption function for an affine cipher if the encryption function is $c = (15p + 13) \bmod 26$?
- Find all pairs of integers keys (a, b) for affine ciphers for which the encryption function $c = (ap + b) \bmod 26$ is the same as the corresponding decryption function.

Show that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

Show that if a, b, c , and d are integers, where $a \neq 0$, such that $a \mid c$ and $b \mid d$, then $ab \mid cd$.

Show that if a, b , and c are integers, where $a \neq 0$ and $c \neq 0$, such that $ac \mid bc$, then $a \mid b$.

Prove or disprove that if $a \mid bc$, where a, b , and c are positive integers and $a \neq 0$, then $a \mid b$ or $a \mid c$.

Show that if a, b, c , and d are integers, where $a \neq 0$, such that $a \mid c$ and $b \mid d$, then $ab \mid cd$.

Show that if a , b , and c are integers, where $a \neq 0$ and $c \neq 0$, such that $ac \mid bc$, then $a \mid b$.

Prove or disprove that if $a \mid bc$, where a , b , and c are positive integers and $a \neq 0$, then $a \mid b$ or $a \mid c$.

Show that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.

Show that if a, b, c , and m are integers such that $m \geq 2$, $c > 0$, and $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$.

Find counterexamples to each of these statements about congruences.

- a) If $ac \equiv bc \pmod{m}$, where a, b, c , and m are integers with $m \geq 2$, then $a \equiv b \pmod{m}$.
- b) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where a, b, c, d , and m are integers with c and d positive and $m \geq 2$, then $a^c \equiv b^d \pmod{m}$.

- Show that if n is an integer then $n^2 \equiv 0$ or $1 \pmod{4}$.

- Show that if n is an integer then $n^2 \equiv 0$ or $1 \pmod{4}$.
- Use Exercise □ to show that if m is a positive integer of the form $4k + 3$ for some nonnegative integer k , then m is not the sum of the squares of two integers.

- Prove that if n is an odd positive integer, then $n^2 \equiv 1 \pmod{8}$.
- Show that if a, b, k , and m are integers such that $k \geq 1$, $m \geq 2$, and $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$.

Determine whether the integers in each of these sets are pairwise relatively prime.

- a) 21, 34, 55
- c) 25, 41, 49, 64

- b) 14, 17, 85
- d) 17, 18, 19, 23

Determine whether the integers in each of these sets are pairwise relatively prime.

- a) 11, 15, 19
- c) 12, 17, 31, 37

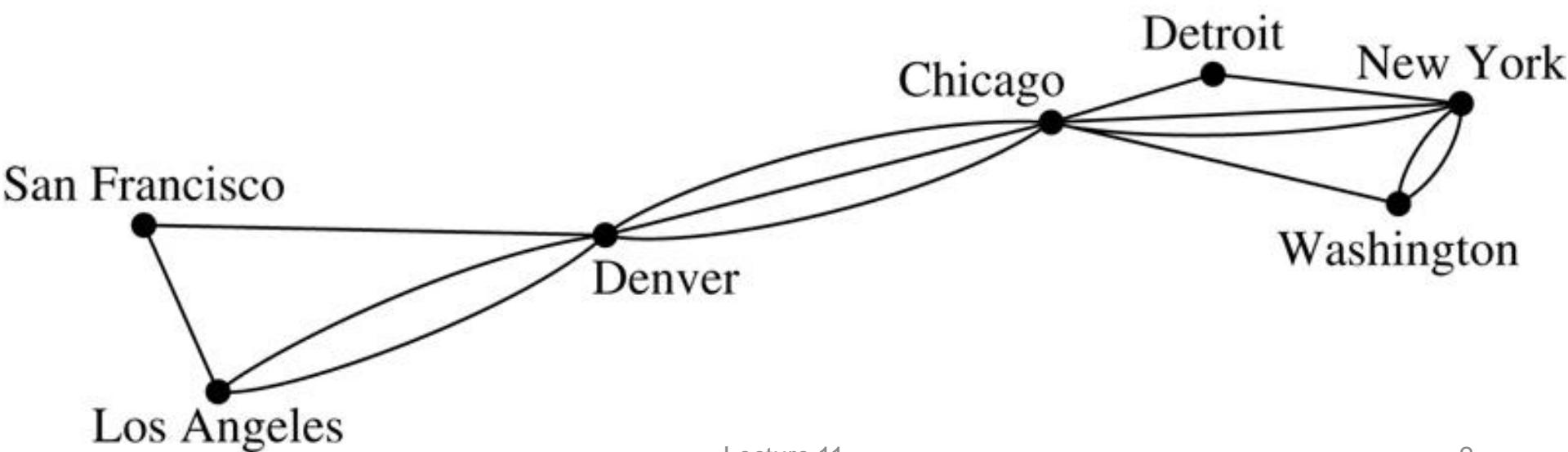
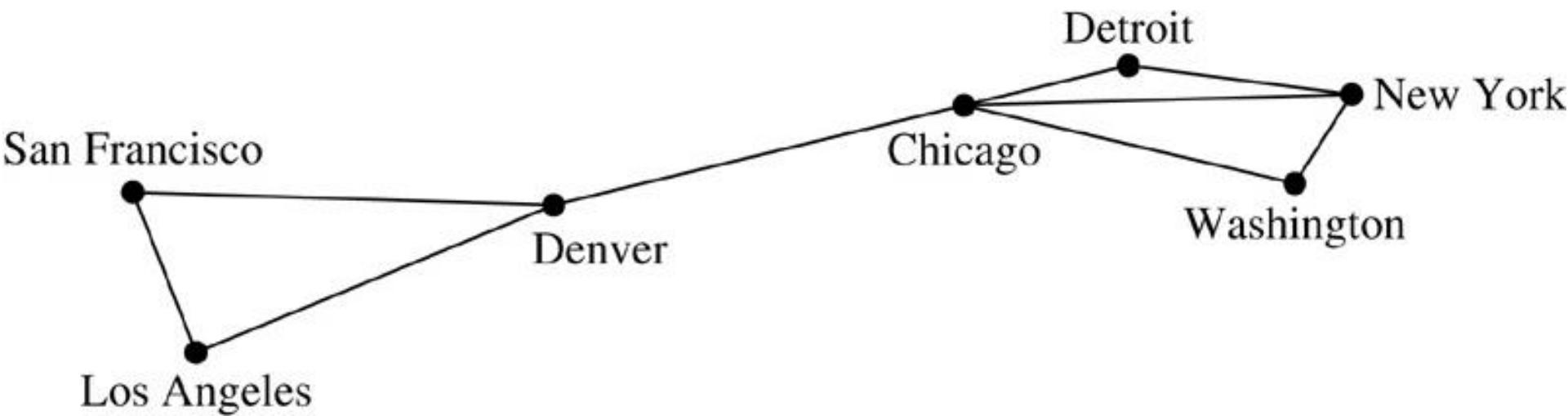
- b) 14, 15, 21
- d) 7, 8, 9, 11

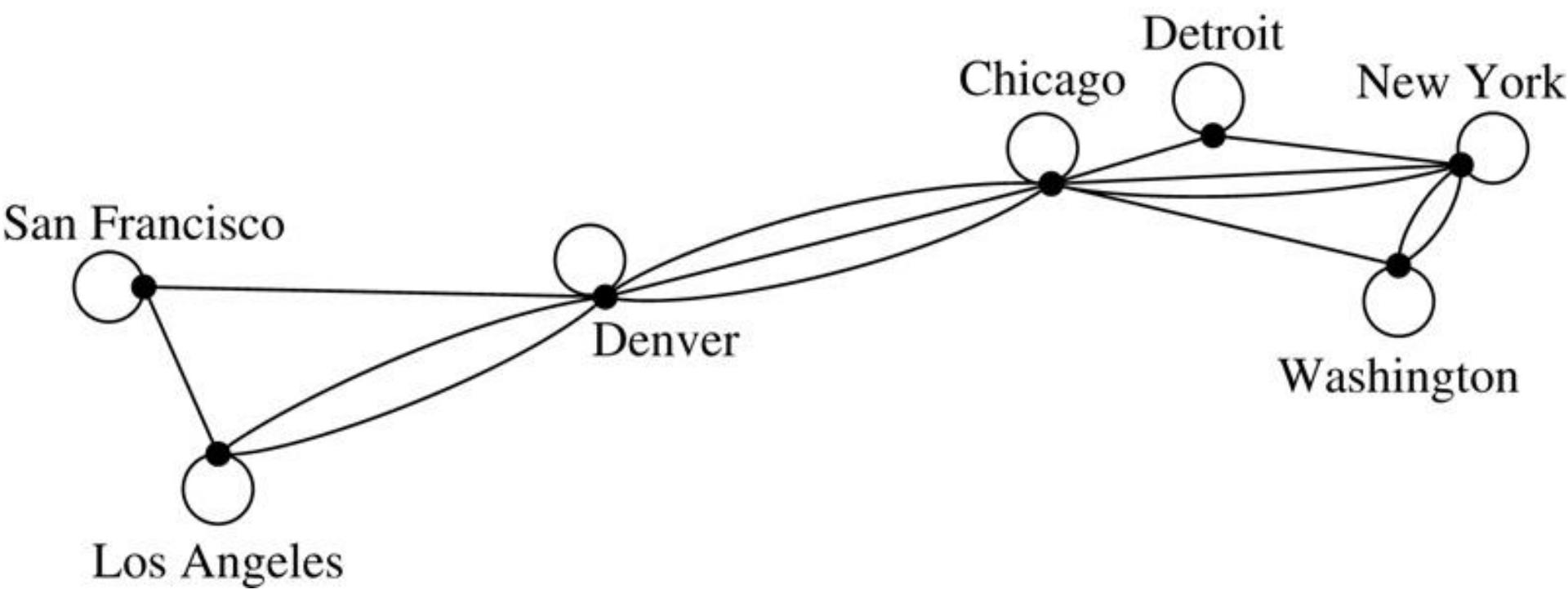
What are the greatest common divisors of these pairs of integers?

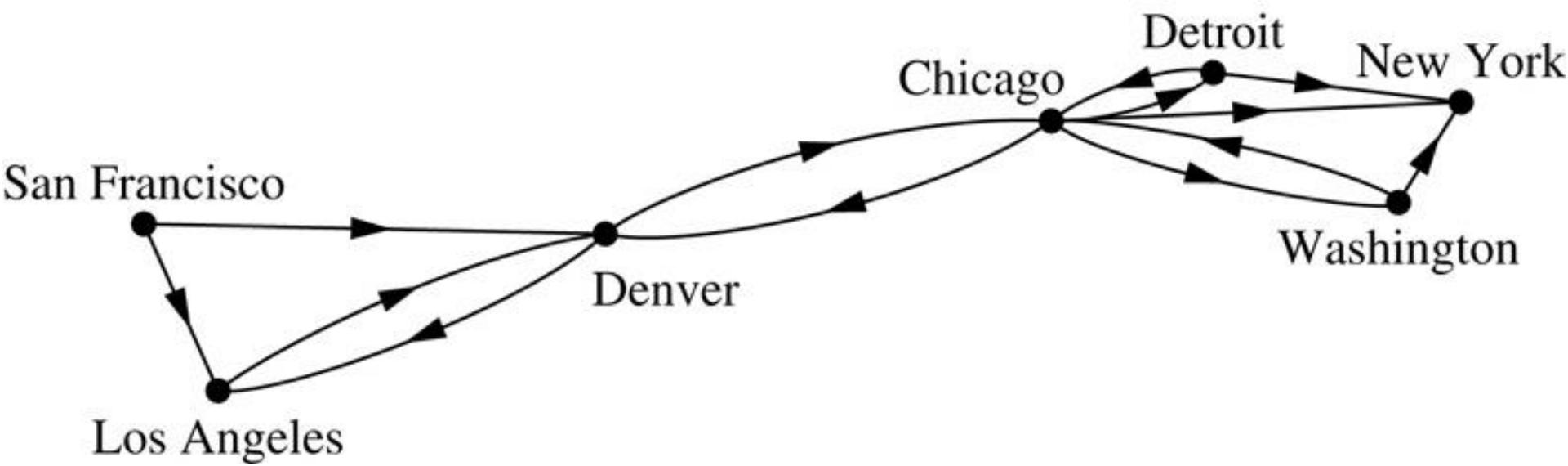
- a) $3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9$
- b) $11 \cdot 13 \cdot 17, 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$
- c) $23^{31}, 23^{17}$
- d) $41 \cdot 43 \cdot 53, 41 \cdot 43 \cdot 53$
- e) $3^{13} \cdot 5^{17}, 2^{12} \cdot 7^{21}$
- f) 1111, 0

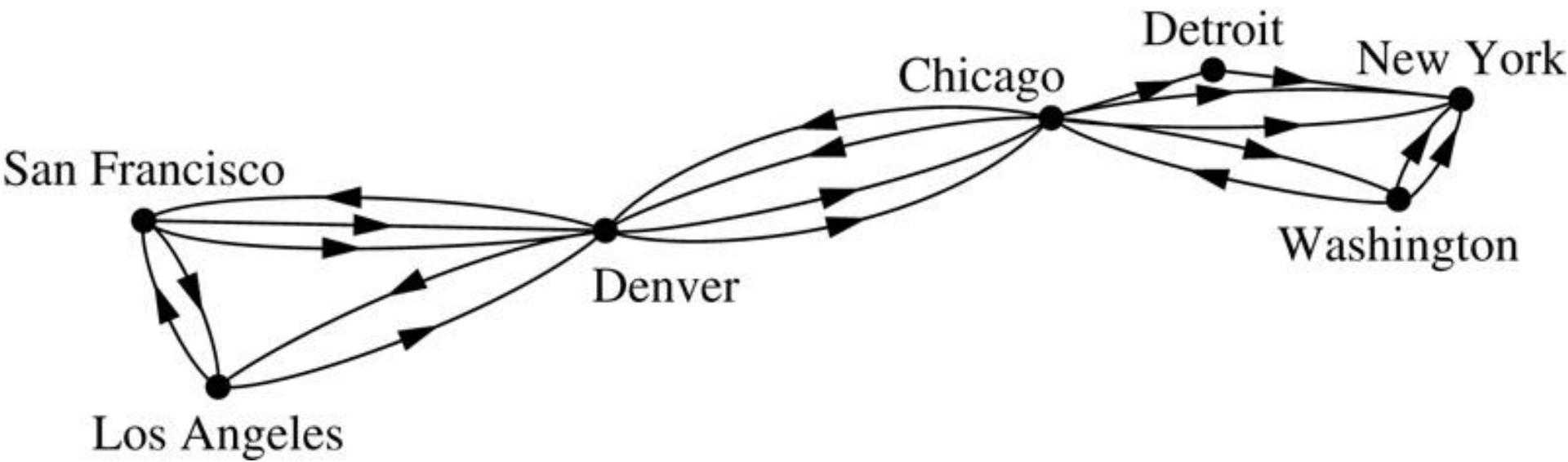
Mat2033 - Discrete Mathematics

Graph Theory and Its Applications



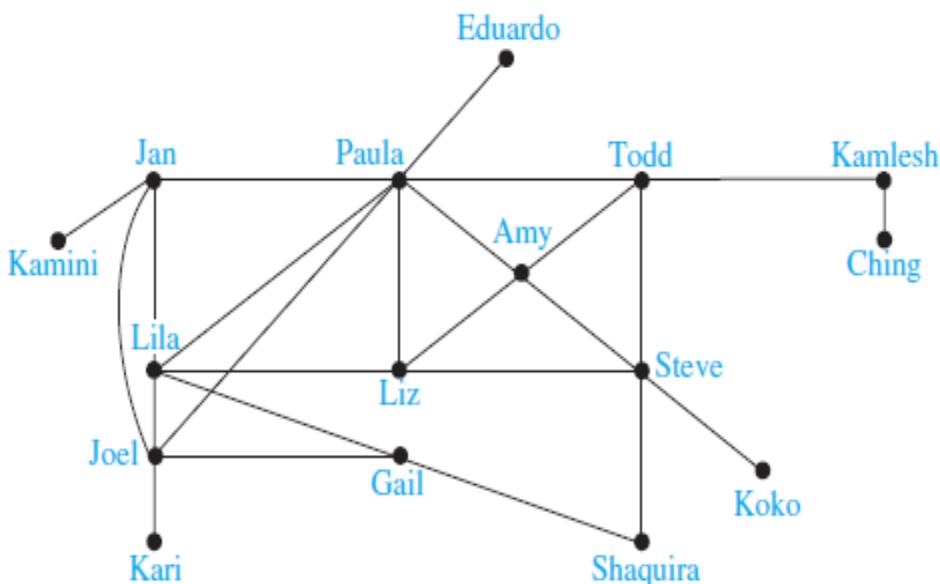






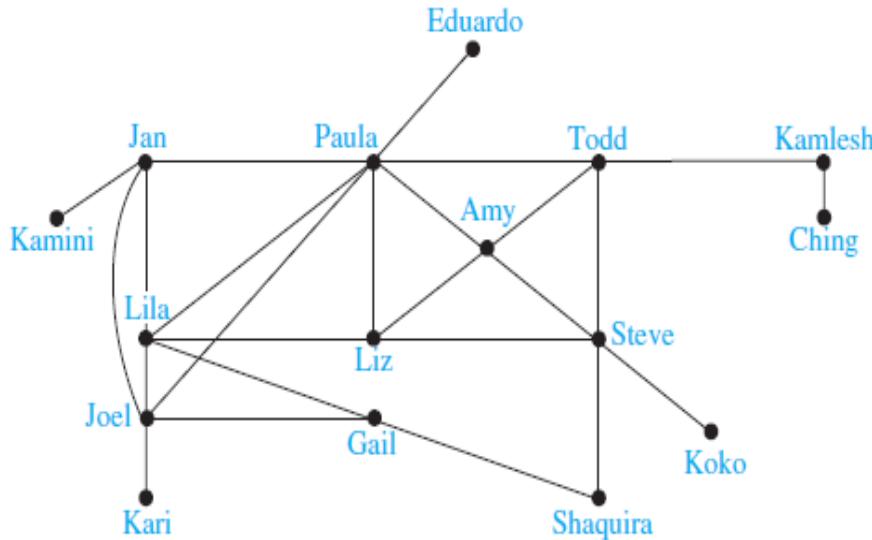
Graph Models

SOCIAL NETWORKS Graphs are extensively used to model social structures based on different kinds of relationships between people or groups of people. These social structures, and the graphs that represent them, are known as **social networks**. In these graph models, individuals or organizations are represented by vertices; relationships between individuals or organizations are represented by edges. The study of social networks is an extremely active multidisciplinary area, and many different types of relationships between people have been studied using them.



An Acquaintanceship Graph.

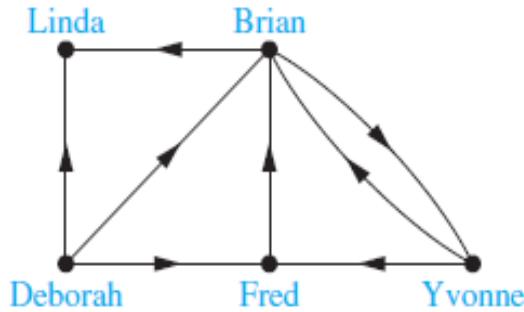
Graph Models



An Acquaintanceship Graph.

Acquaintanceship and Friendship Graphs We can use a simple graph to represent whether two people know each other, that is, whether they are acquainted, or whether they are friends (either in the real world in the virtual world via a social networking site such as Facebook). Each person in a particular group of people is represented by a vertex. An undirected edge is used to connect two people when these people know each other, when we are concerned only with acquaintanceship, or whether they are friends. No multiple edges and usually no loops are used. (If we want to include the notion of self-knowledge, we would include loops.) A small acquaintanceship graph is shown in Figure . The acquaintanceship graph of all people in the world has more than six billion vertices and probably more than one trillion edges!

Graph Models



An Influence Graph.

Influence Graphs In studies of group behavior it is observed that certain people can influence the thinking of others. A directed graph called an **influence graph** can be used to model this behavior. Each person of the group is represented by a vertex. There is a directed edge from vertex a to vertex b when the person represented by vertex a can influence the person represented by vertex b . This graph does not contain loops and it does not contain multiple directed edges. An example of an influence graph for members of a group is shown in Figure . In the group modeled by this influence graph, Deborah cannot be influenced, but she can influence Brian, Fred, and Linda. Also, Yvonne and Brian can influence each other.

Graph Models

COMMUNICATION NETWORKS We can model different communications networks using vertices to represent devices and edges to represent the particular type of communications links of interest. We have already modeled a data network in the first part of this section.

Call Graphs Graphs can be used to model telephone calls made in a network, such as a long-distance telephone network. In particular, a directed multigraph can be used to model calls where each telephone number is represented by a vertex and each telephone call is represented by a directed edge. The edge representing a call starts at the telephone number from which the call was made and ends at the telephone number to which the call was made. We need directed edges because the direction in which the call is made matters. We need multiple directed edges because we want to represent each call made from a particular telephone number to a second number.

A small telephone call graph is displayed in Figure 8(a), representing seven telephone numbers. This graph shows, for instance, that three calls have been made from 732-555-1234 to 732-555-9876 and two in the other direction, but no calls have been made from 732-555-4444 to any of the other six numbers except 732-555-0011. When we care only whether there has been a call connecting two telephone numbers, we use an undirected graph with an edge connecting telephone numbers when there has been a call between these numbers. This version of the call graph is displayed in Figure 8(b).

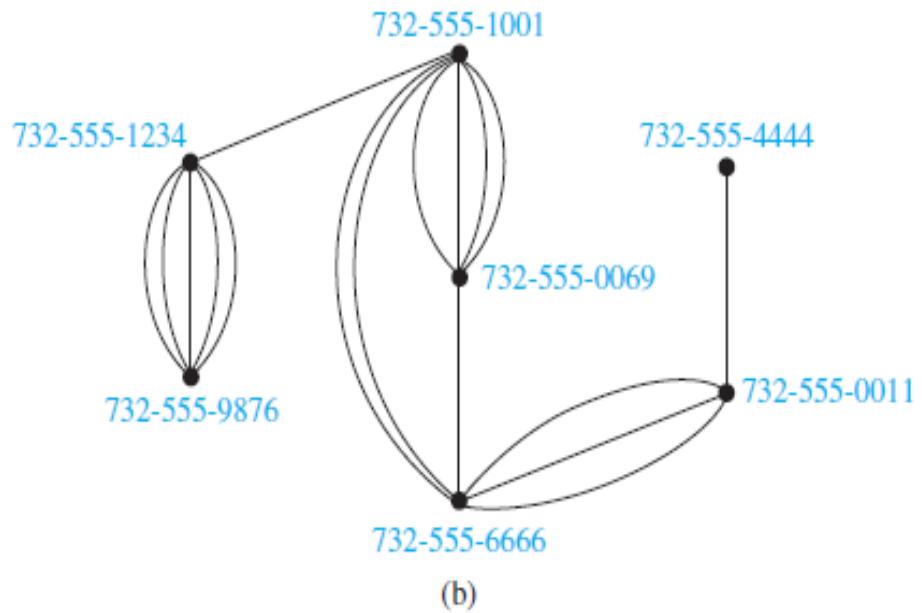
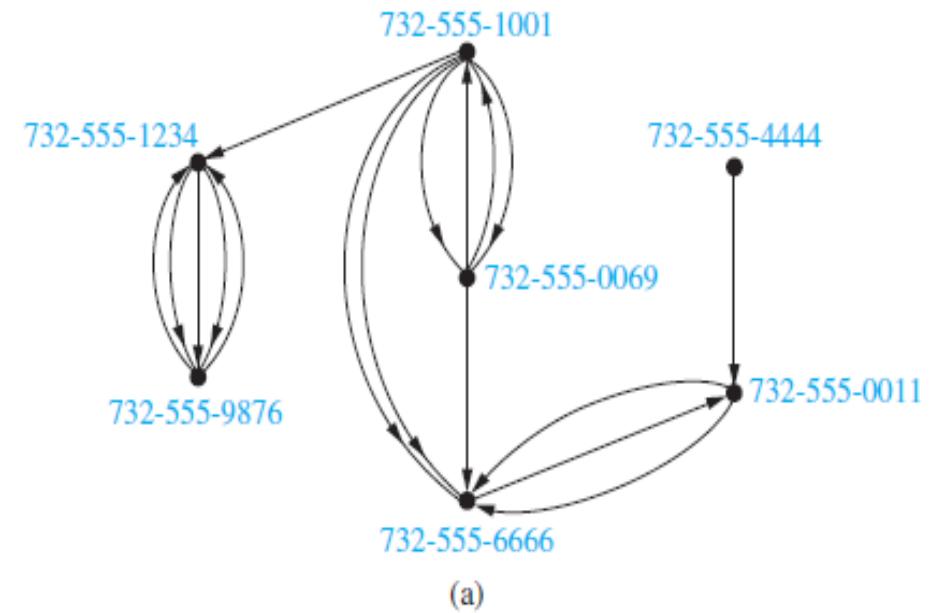


FIGURE 8 A Call Graph.

Graph Models

INFORMATION NETWORKS Graphs can be used to model various networks that link particular types of information. Here, we will describe how to model the World Wide Web using a graph. We will also describe how to use a graph to model the citations in different types of documents.

The Web Graph The World Wide Web can be modeled as a directed graph where each Web page is represented by a vertex and where an edge starts at the Web page a and ends at the Web page b if there is a link on a pointing to b . Because new Web pages are created and others removed somewhere on the Web almost every second, the Web graph changes on an almost continual basis. Many people are studying the properties of the Web graph to better understand the nature of the Web.

Citation Graphs Graphs can be used to represent citations in different types of documents, including academic papers, patents, and legal opinions. In such graphs, each document is represented by a vertex, and there is an edge from one document to a second document if the first document cites the second in its citation list. (In an academic paper, the citation list is the bibliography, or list of references; in a patent it is the list of previous patents that are cited; and in a legal opinion it is the list of previous opinions cited.) A citation graph is a directed graph without loops or multiple edges.

Graph Models

TRANSPORTATION NETWORKS We can use graphs to model many different types of transportation networks, including road, air, and rail networks, as well shipping networks.

Airline Routes We can model airline networks by representing each airport by a vertex. In particular, we can model all the flights by a particular airline each day using a directed edge to represent each flight, going from the vertex representing the departure airport to the vertex representing the destination airport. The resulting graph will generally be a directed multigraph, as there may be multiple flights from one airport to some other airport during the same day. ◀

Road Networks Graphs can be used to model road networks. In such models, vertices represent intersections and edges represent roads. When all roads are two-way and there is at most one road connecting two intersections, we can use a simple undirected graph to model the road network. However, we will often want to model road networks when some roads are one-way and when there may be more than one road between two intersections. To build such models, we use undirected edges to represent two-way roads and we use directed edges to represent one-way roads. Multiple undirected edges represent multiple two-way roads connecting the same two intersections. Multiple directed edges represent multiple one-way roads that start at one intersection and end at a second intersection. Loops represent loop roads. Mixed graphs are needed to model road networks that include both one-way and two-way roads. ◀

BIOLOGICAL NETWORKS Many aspects of the biological sciences can be modeled using graphs.

Niche Overlap Graphs in Ecology Graphs are used in many models involving the interaction of different species of animals. For instance, the competition between species in an ecosystem can be modeled using a **niche overlap graph**. Each species is represented by a vertex. An undirected edge connects two vertices if the two species represented by these vertices compete (that is, some of the food resources they use are the same). A niche overlap graph is a simple graph because no loops or multiple edges are needed in this model. The graph in Figure 11 models the ecosystem of a forest. We see from this graph that squirrels and raccoons compete but that crows and shrews do not.

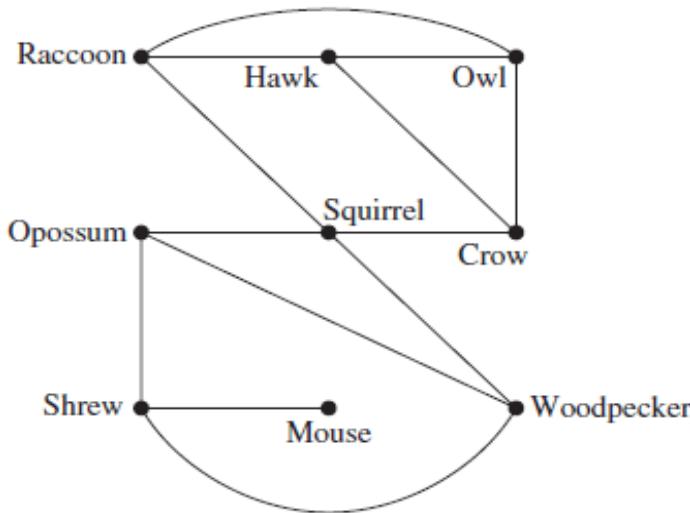


FIGURE 11 A Niche Overlap Graph.

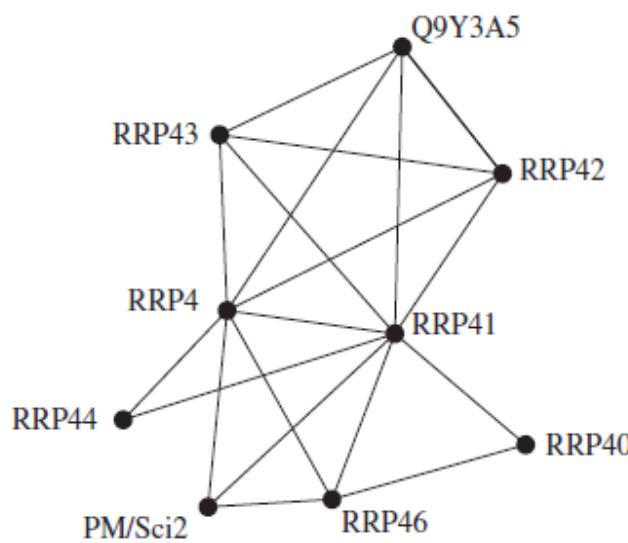


FIGURE 12 A Module of a Protein Interaction Graph.

Protein Interaction Graphs A protein interaction in a living cell occurs when two or more proteins in that cell bind to perform a biological function. Because protein interactions are crucial for most biological functions, many scientists work on discovering new proteins and understanding interactions between proteins. Protein interactions within a cell can be modeled using a **protein interaction graph** (also called a **protein–protein interaction network**), an undirected graph in which each protein is represented by a vertex, with an edge connecting the vertices representing each pair of proteins that interact. It is a challenging problem to determine genuine protein interactions in a cell, as experiments often produce false positives, which conclude that two proteins interact when they really do not. Protein interaction graphs can be used to deduce important biological information, such as by identifying the most important proteins for various functions and the functionality of newly discovered proteins.

Because there are thousands of different proteins in a typical cell, the protein interaction graph of a cell is extremely large and complex. For example, yeast cells have more than 6,000 proteins, and more than 80,000 interactions between them are known, and human cells have more than 100,000 proteins, with perhaps as many as 1,000,000 interactions between them. Additional vertices and edges are added to a protein interaction graph when new proteins and interactions between proteins are discovered. Because of the complexity of protein interaction graphs, they are often split into smaller graphs called modules that represent groups of proteins that are involved in a particular function of a cell. Figure 12 illustrates a module of the protein interaction graph described in [Bo04], comprising the complex of proteins that degrade RNA in human cells. To learn more about protein interaction graphs, see [Bo04], [Ne10], and [Hu07].

Graph Models

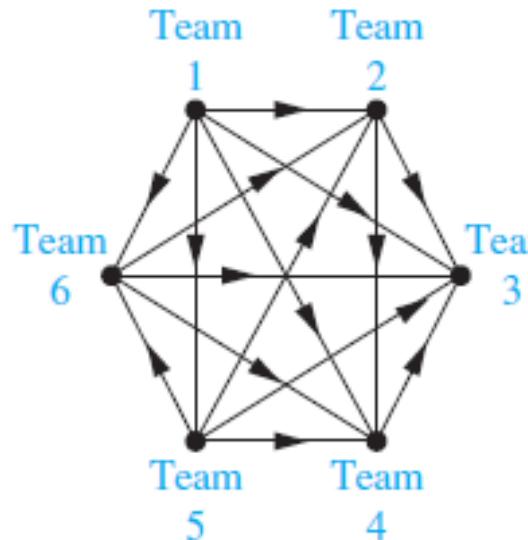


FIGURE 13 A Graph Model of a Round-Robin Tournament.

TOURNAMENTS We now give some examples that show how graphs can also be used to model different kinds of tournaments.

Round-Robin Tournaments A tournament where each team plays every other team exactly once and no ties are allowed is called a **round-robin tournament**. Such tournaments can be modeled using directed graphs where each team is represented by a vertex. Note that (a, b) is an edge if team a beats team b . This graph is a simple directed graph, containing no loops or multiple directed edges (because no two teams play each other more than once). Such a directed graph model is presented in Figure 13. We see that Team 1 is undefeated in this tournament, and Team 3 is winless.

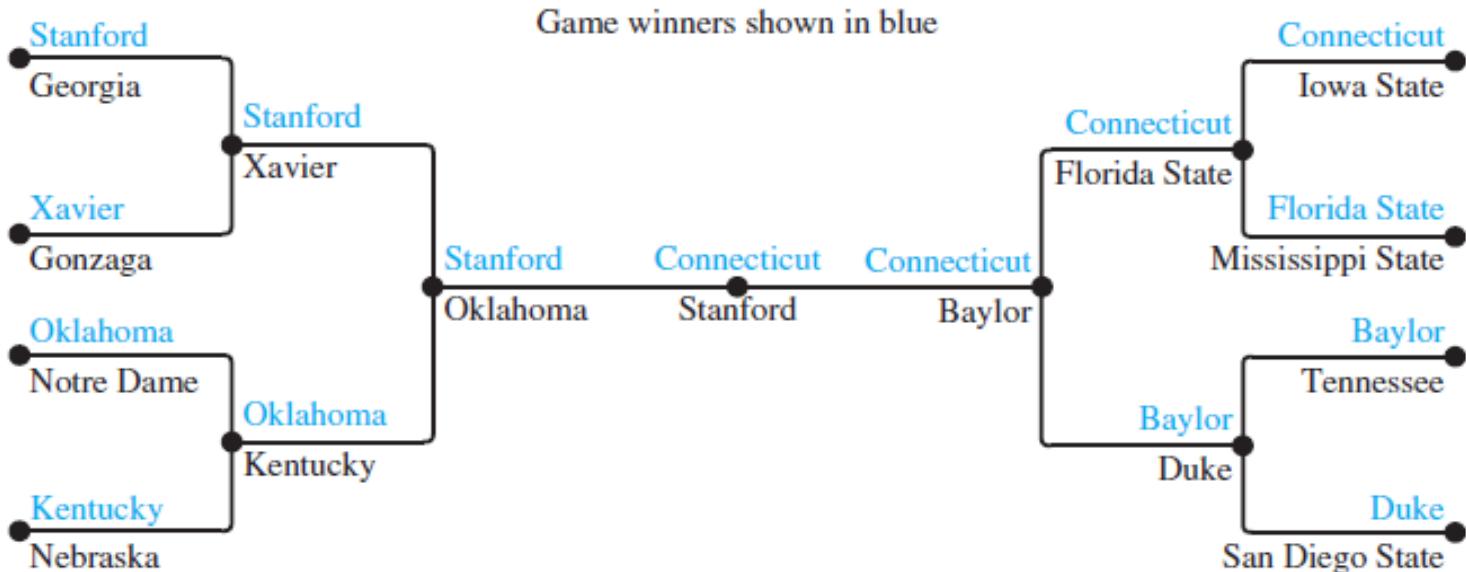


FIGURE 14 A Single-Elimination Tournament.

Single-Elimination Tournaments A tournament where each contestant is eliminated after one loss is called a **single-elimination tournament**. Single-elimination tournaments are often used in sports, including tennis championships and the yearly NCAA basketball championship. We can model such a tournament using a vertex to represent each game and a directed edge to connect a game to the next game the winner of this game played in. The graph in Figure 14 represents the games played by the final 16 teams in the 2010 NCAA women's basketball tournament. ◀

Definition of a graph

- A **graph** G is a finite nonempty set $V(G)$ of **vertices** (also called **nodes**) and a (possibly empty) set $E(G)$ of 2-element subsets of $V(G)$ called **edges** (or **lines**).

$V(G)$: vertex set of G

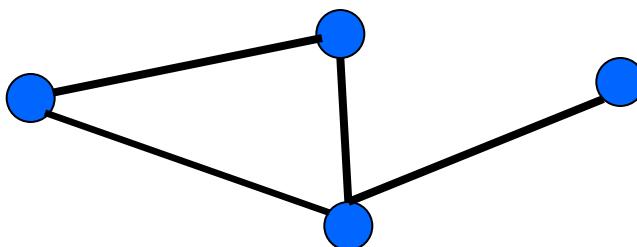
$E(G)$: edge set of G

edge : $\{u, v\} = \{v, u\} = uv$ (or vu)

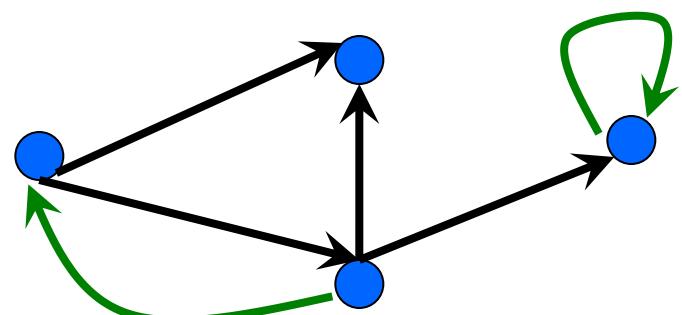
G **directed graph** (digraph) edge: (u,v)

Types of Graphs

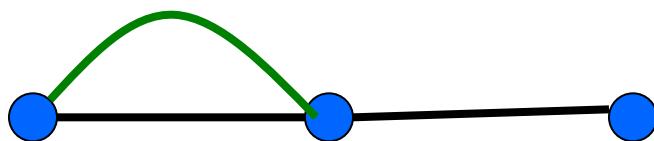
Simple
Graph



Directed Graph



Multi-Graph



Most of the
problems in
this course.

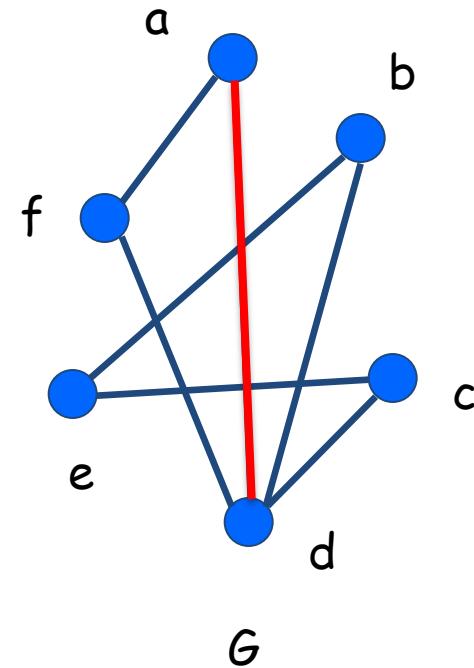
Simple Graphs

A graph $G=(V,E)$ consists of:

A set of vertices, V

A set of *undirected* edges, E

- $V(G) = \{a,b,c,d,e,f\}$
- $E(G) = \{ad, af, bd, be, cd, ce, df\}$



Two vertices a,d are **adjacent (neighbours)** if the edge ad is present.

Example

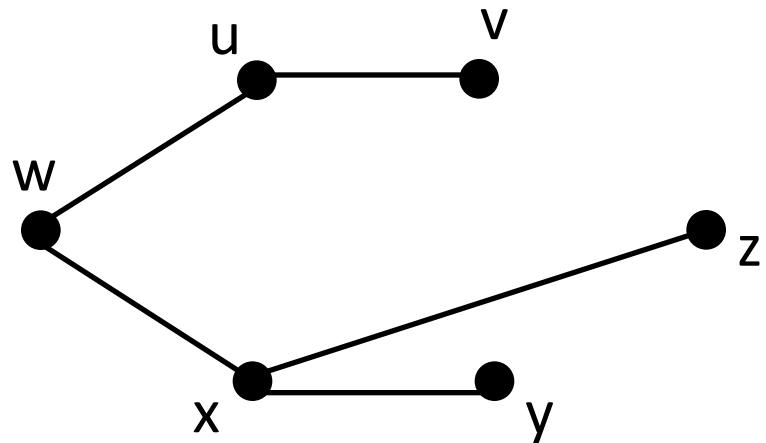
- A graph $G=(V,E)$, where

$$V=\{u, v, w, x, y, z\}$$

$$E=\{\{u,v\}, \{u,w\}, \{w,x\}, \{x,y\}, \{x,z\}\}$$

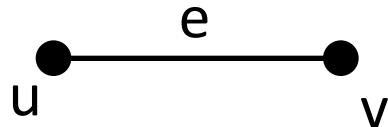
$$E=\{uv, uw, wx, xy, xz\}$$

- G diagram :



Adjacent and Incident

- u, v : vertices of a graph G



- u and v are adjacent in G if $uv \in E(G)$
(u is adjacent to v , v is adjacent to u)
- $e=uv$ (e joins u and v) (e is incident with u , e is incident with v)

Graphs types

- undirected graph:

loop



multiedges, parallel edges



- (simple) graph: loop (✗), multiedge (✗)
- multigraph: loop (✗), multiedge (✓)
- Pseudograph: loop (✓), multiedge (✓)

order and size

- The number of vertices in a graph G is called its **order** (denoted by $|V(G)|$).
- The number of edges is its **size** (denoted by $|E(G)|$).
- Proposition 1:
If $|V(G)| = p$ and $|E(G)| = q$, then $q \leq \binom{p}{2}$
- A graph of order p and size q is called a **(p, q) graph**.

Application of graphs

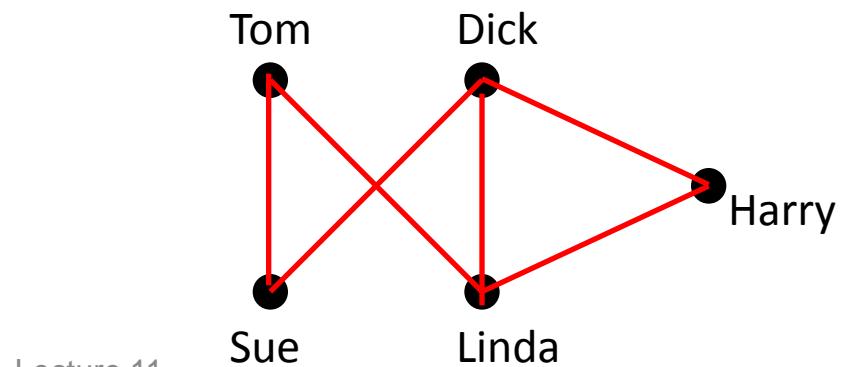
Example:

Tom, Dick know Sue, Linda.

Harry knows Dick and Linda.

⇒

acquaintance graph:



The degree of a vertex

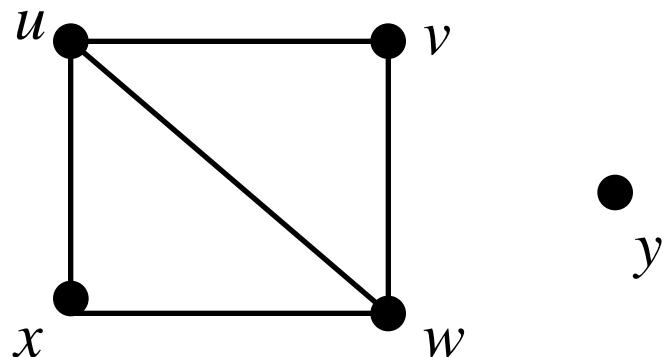
Definition.

For a vertex v of G , its neighborhood

$$N(v) = \{ u \in V(G) \mid vu \in E(G) \}.$$

The degree of vertex v is

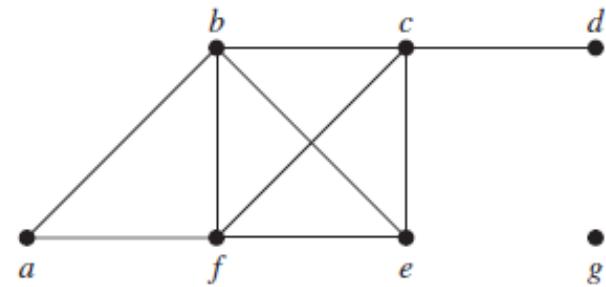
$$\deg(v) = | N(v) |.$$



$$N(u) = \{x, w, v\}, \quad N(y) = \{\}$$
$$\deg(u) = 3, \deg(y) = 0$$

Notes

- If $|V(G)| = p$, then $0 \leq \deg(v) \leq p-1$, $\forall v \in V(G)$.
- If $\deg(v) = 0$, then v is called an **isolated vertex**
- If $\deg(v) = 1$, then v is called an **pendant vertex**
- v is an **odd vertex** if $\deg(v)$ is odd.
 v is an **even vertex** if $\deg(v)$ is even.

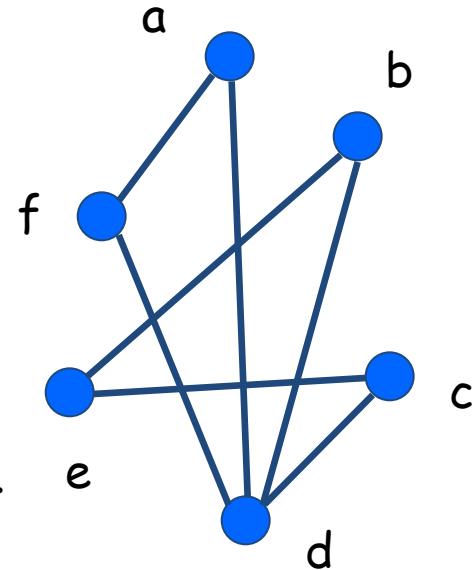


Vertex Degrees

An edge uv is **incident** on the vertex u and the vertex v .

The **neighbour set** $N(v)$ of a vertex v is the set of vertices adjacent to it.

e.g. $N(a) = \{d, f\}$, $N(d) = \{a, b, c, f\}$, $N(e) = \{b, c\}$.



degree of a vertex = # of **incident** edges

e.g. $\deg(d) = 4$, $\deg(a)=\deg(b)=\deg(c)=\deg(e)=\deg(f)=2$.

the degree of a vertex v = the number of neighbours of v ?

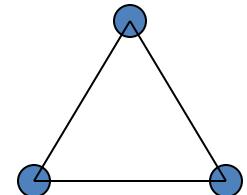
For multigraphs, **NO**.

For simple graphs, **YES**.

Degree Sequence

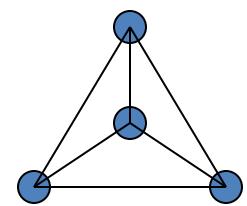
Is there a graph with degree sequence $(2,2,2)$?

YES.



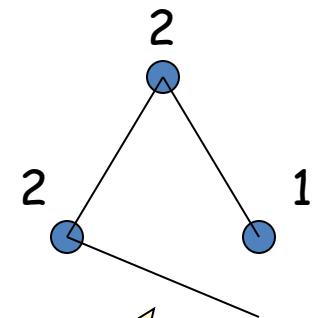
Is there a graph with degree sequence $(3,3,3,3)$?

YES.



Is there a graph with degree sequence $(2,2,1)$?

NO.



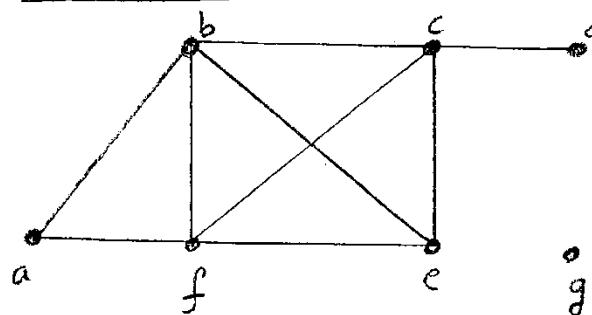
Is there a graph with degree sequence $(2,2,2,2,1)$?

NO.

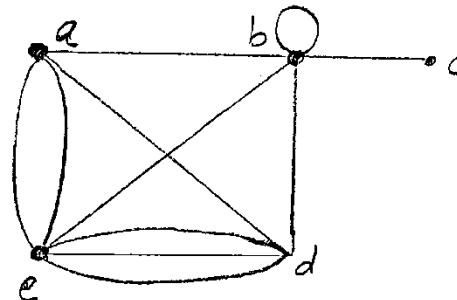
What's wrong with these sequences?

Where to go?

Example:



G



H

What are the degrees of the vertices in the graphs G and H?

The *degree of a vertex in an undirected graph* is the number of edges incident with it, except that a loop at a vertex contributes twice to the degree of that vertex. The degree of the vertex v is denoted by $\deg(v)$.

Solution: In G, $\deg(a)=2$, $\deg(b)=\deg(c)=\deg(f)=4$,
 $\deg(d)=1$, $\deg(e)=3$, $\deg(g)=0$.

In H, $\deg(a)=4$, $\deg(b)=\deg(c)=1$,
and $\deg(d)=5$.

Handshaking Lemma

For any graph, sum of degrees = twice # edges

Lemma.

$$2|E| = \sum_{v \in V} \deg(v)$$

Corollary.

1. Sum of degree is an even number.
2. Number of odd degree vertices is even.

Examples.

$2+2+1 = \text{odd}$, so impossible.

$2+2+2+2+1 = \text{odd}$, so impossible.

Handshaking Lemma

Lemma.

$$2|E| = \sum_{v \in V} \deg(v)$$

Proof. Each edge contributes 2 to the sum on the right.

Question. Given a degree sequence, if the sum of degree is even, is it true that there is a graph with such a degree sequence?

For simple graphs, **NO**, consider the degree sequence (3,3,3,1).

For multigraphs (with self loops), **YES!** (easy by induction)

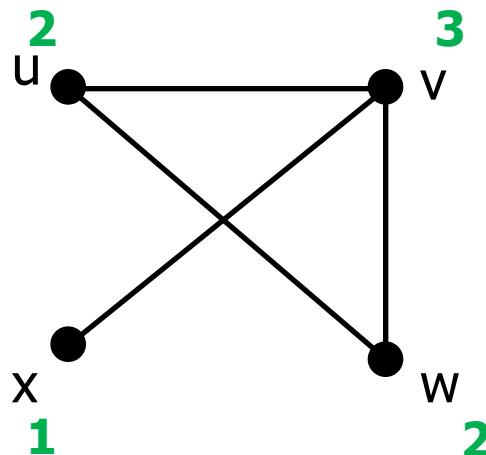
Handshaking theorem

- **Theorem 1.1 (Handshaking theorem)**

Let G be a graph, then

$$\sum_{v \in V(G)} \deg(v) = |E(G)| \times 2$$

Example:



$$\sum_{v \in V(G)} \deg(v) = 8$$

$$|E(G)| = 4$$

Handshaking theorem

Corollary 1.1

Every graph contains an even number of odd vertices.

Proof: If the number of vertices with odd degree is odd, then the degree sum must be odd. →←

Example: How many edges are there in a graph with 10 vertices each of degree 6?

Example: How many edges are there in a graph with 10 vertices each of degree 6?

Solution:

$$\text{Sum of degrees of vertices} = 6 \cdot 10 = 60$$

$$2e = 60 \Rightarrow e = \frac{60}{2} = 30 \text{ edges.}$$

Example: A certain graph G has order 14 and size 27.

The degree of each vertex of G is 3, 4 or 5.

There are six vertices of degree 4.

How many vertices of G have degree 3 and how many have degree 5 ?

Solution: Let x be the number of vertices of G having degree 3.

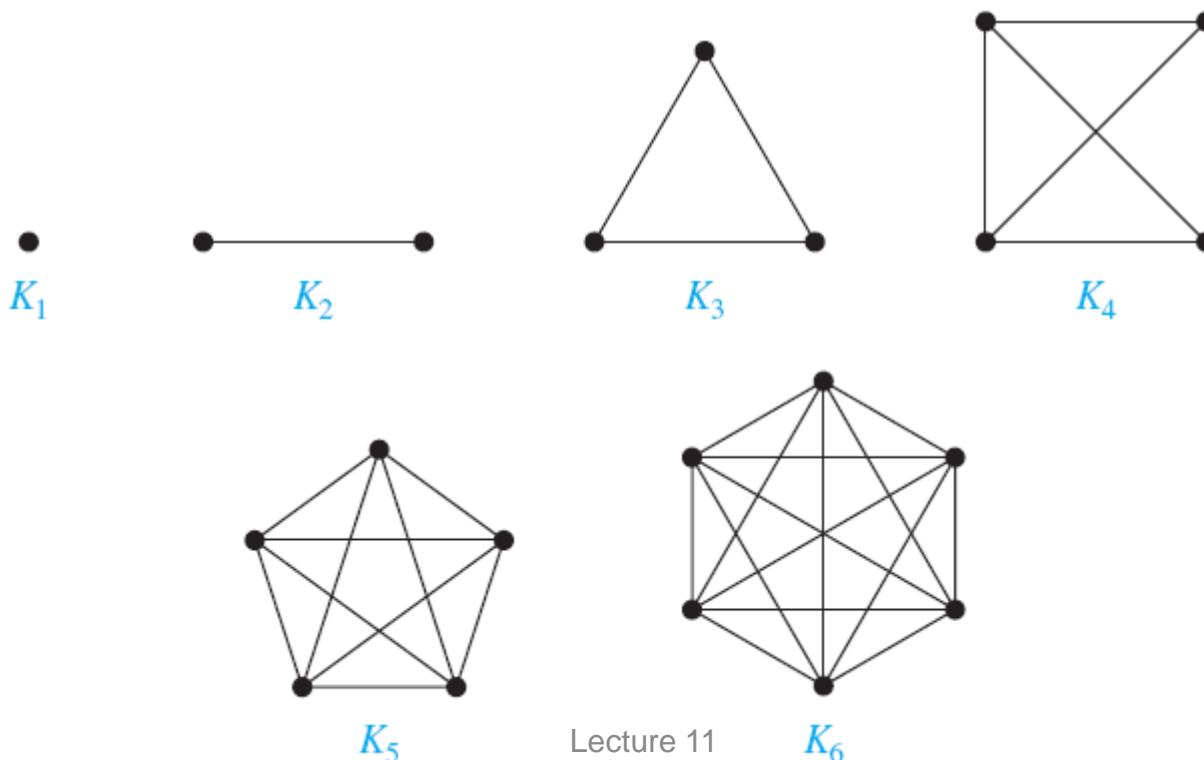
$14 - 6 = 8$ vertices have degree 3 or 5. So there are $8 - x$ vertices of degree 5.

Then we have $3 \cdot x + 4 \cdot 6 + 5 \cdot (8 - x) = 2 \cdot 27$

Hence $x = 5$, $8 - x = 3$

Some Special Simple Graphs

Complete Graphs A **complete graph on n vertices**, denoted by K_n , is a simple graph that contains exactly one edge between each pair of distinct vertices. The graphs K_n , for $n = 1, 2, 3, 4, 5, 6$, are displayed in Figure 3. A simple graph for which there is at least one pair of distinct vertex not connected by an edge is called **noncomplete**. 



Cycles A **cycle** C_n , $n \geq 3$, consists of n vertices v_1, v_2, \dots, v_n and edges $\{v_1, v_2\}$, $\{v_2, v_3\}, \dots, \{v_{n-1}, v_n\}$, and $\{v_n, v_1\}$. The cycles C_3 , C_4 , C_5 , and C_6 are displayed in Figure 4. 

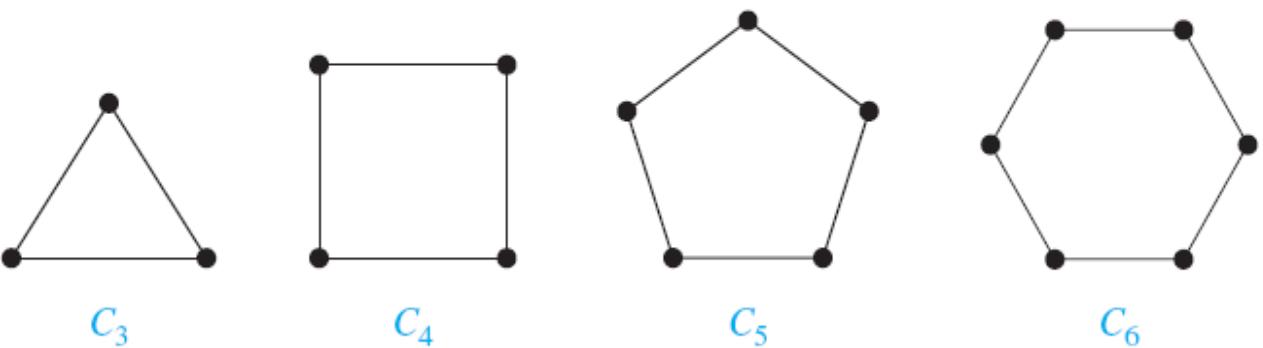


FIGURE 4 The Cycles C_3 , C_4 , C_5 , and C_6 .

Wheels We obtain a **wheel** W_n when we add an additional vertex to a cycle C_n , for $n \geq 3$, and connect this new vertex to each of the n vertices in C_n , by new edges. The wheels W_3 , W_4 , W_5 , and W_6 are displayed in Figure 5.

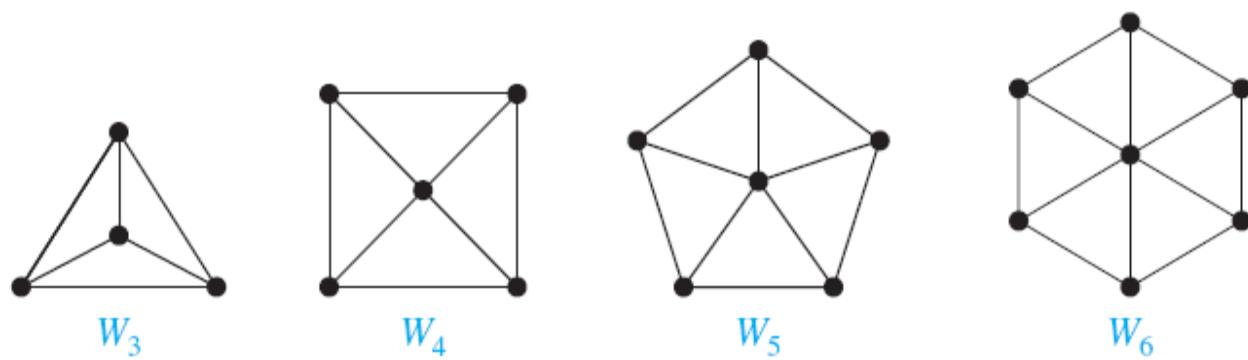


FIGURE 5 The Wheels W_3 , W_4 , W_5 , and W_6 .

n -Cubes An **n -dimensional hypercube**, or **n -cube**, denoted by Q_n , is a graph that has vertices representing the 2^n bit strings of length n . Two vertices are adjacent if and only if the bit strings that they represent differ in exactly one bit position. We display Q_1 , Q_2 , and Q_3 in Figure 6.

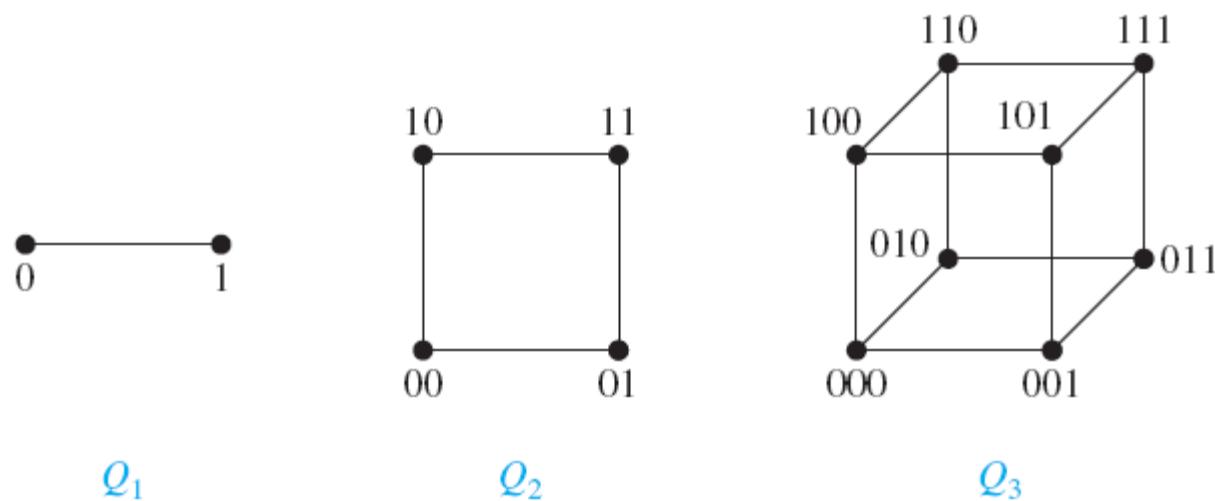


FIGURE 6 The n -cube Q_n , $n = 1, 2, 3$.

Note that you can construct the $(n + 1)$ -cube Q_{n+1} from the n -cube Q_n by making two copies of Q_n , prefacing the labels on the vertices with a 0 in one copy of Q_n and with a 1 in the other copy of Q_n , and adding edges connecting two vertices that have labels differing only in the first bit. In Figure 6, Q_3 is constructed from Q_2 by drawing two copies of Q_2 as the top and bottom faces of Q_3 , adding 0 at the beginning of the label of each vertex in the bottom face and 1 at the beginning of the label of each vertex in the top face. (Here, by *face* we mean a face of a cube in three-dimensional space. Think of drawing the graph Q_3 in three-dimensional space with copies of Q_2 as the top and bottom faces of a cube and then drawing the projection of the resulting depiction in the plane.) ◀

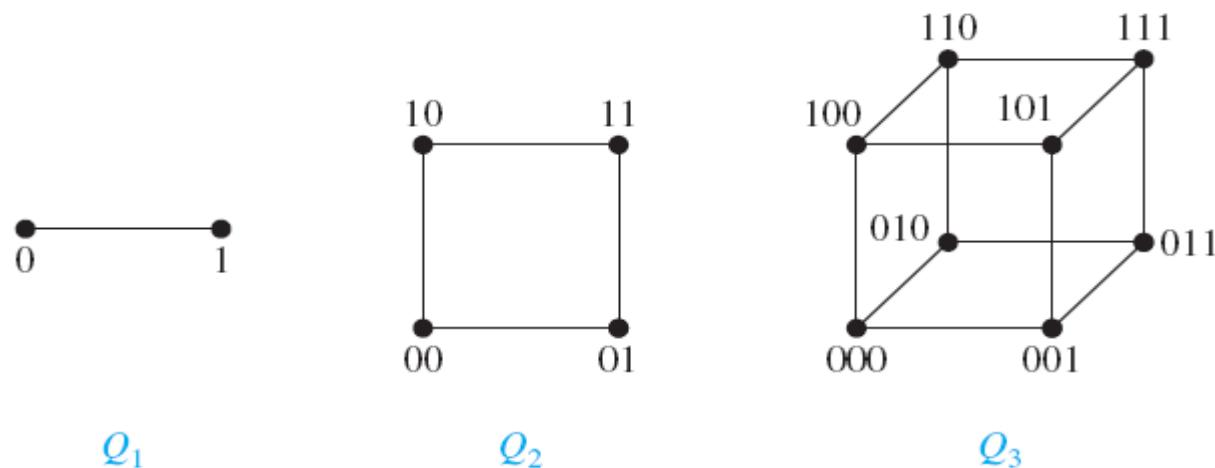


FIGURE 6 The n -cube Q_n , $n = 1, 2, 3$.

Mat2033 - Discrete Mathematics

Graph Theory and Its Applications

Definition of a graph

- A **graph** G is a finite nonempty set $V(G)$ of **vertices** (also called **nodes**) and a (possibly empty) set $E(G)$ of 2-element subsets of $V(G)$ called **edges** (or **lines**).

$V(G)$: vertex set of G

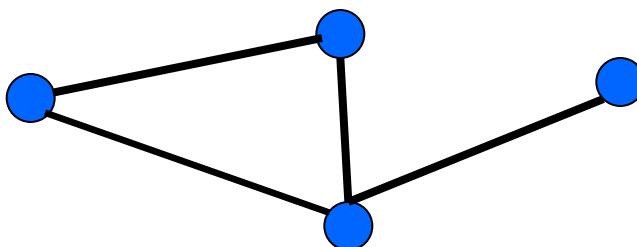
$E(G)$: edge set of G

edge : $\{u, v\} = \{v, u\} = uv$ (or vu)

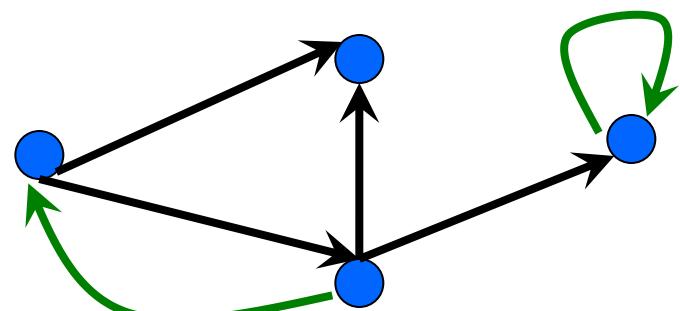
G **directed graph** (digraph) edge: (u,v)

Types of Graphs

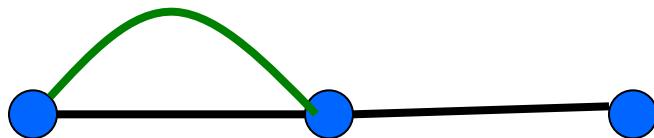
Simple
Graph



Directed Graph



Multi-Graph



Most of the
problems in
this course.

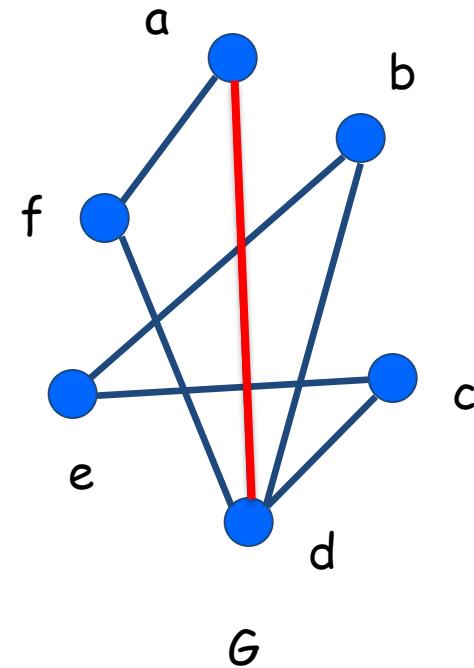
Simple Graphs

A graph $G=(V,E)$ consists of:

A set of vertices, V

A set of *undirected* edges, E

- $V(G) = \{a,b,c,d,e,f\}$
- $E(G) = \{ad, af, bd, be, cd, ce, df\}$



Two vertices a,d are **adjacent (neighbours)** if the edge ad is present.

Example

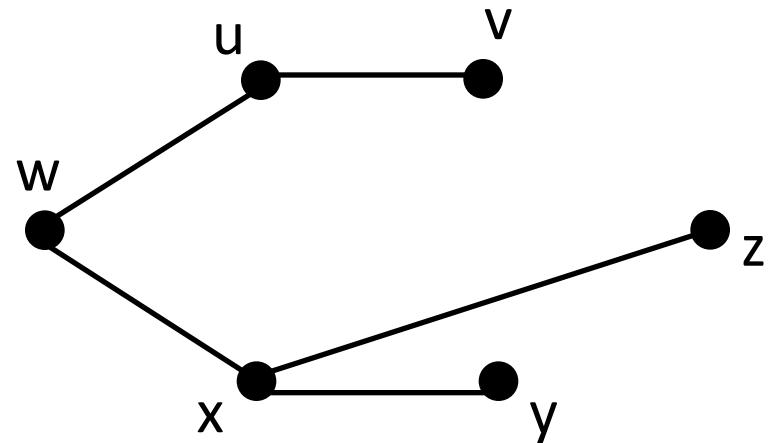
- A graph $G=(V,E)$, where

$$V=\{u, v, w, x, y, z\}$$

$$E=\{\{u,v\}, \{u,w\}, \{w,x\}, \{x,y\}, \{x,z\}\}$$

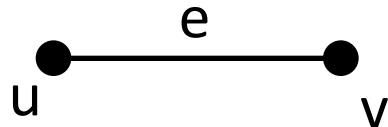
$$E=\{uv, uw, wx, xy, xz\}$$

- G diagram :



Adjacent and Incident

- u, v : vertices of a graph G



- u and v are adjacent in G if $uv \in E(G)$
(u is adjacent to v , v is adjacent to u)
- $e=uv$ (e joins u and v) (e is incident with u , e is incident with v)

Graphs types

- undirected graph:

loop



multiedges, parallel edges



- (simple) graph: loop (✗), multiedge (✗)
- multigraph: loop (✗), multiedge (✓)
- Pseudograph: loop (✓), multiedge (✓)

order and size

- The number of vertices in a graph G is called its **order** (denoted by $|V(G)|$).
- The number of edges is its **size** (denoted by $|E(G)|$).
- Proposition 1:
If $|V(G)| = p$ and $|E(G)| = q$, then $q \leq \binom{p}{2}$
- A graph of order p and size q is called a **(p, q) graph**.

Application of graphs

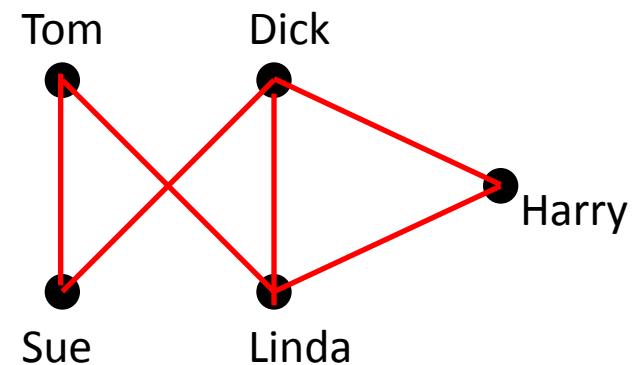
Example:

Tom, Dick know Sue, Linda.

Harry knows Dick and Linda.

⇒

acquaintance graph:



The degree of a vertex

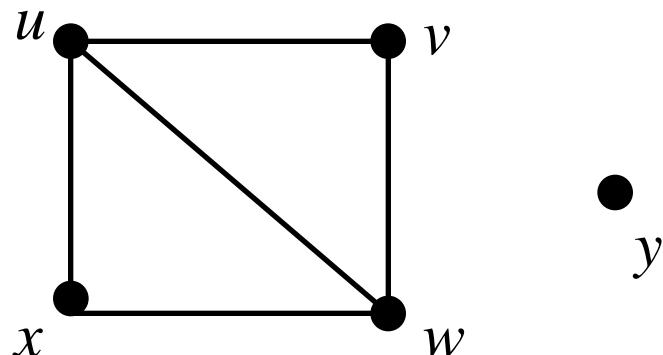
Definition.

For a vertex v of G , its neighborhood

$$N(v) = \{ u \in V(G) \mid vu \in E(G) \}.$$

The degree of vertex v is

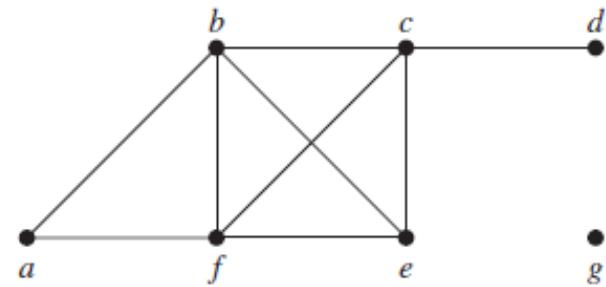
$$\deg(v) = | N(v) |.$$



$$N(u) = \{x, w, v\}, \quad N(y) = \{\}$$
$$\deg(u) = 3, \deg(y) = 0$$

Notes

- If $|V(G)| = p$, then $0 \leq \deg(v) \leq p-1$, $\forall v \in V(G)$.
- If $\deg(v) = 0$, then v is called an **isolated vertex**
- If $\deg(v) = 1$, then v is called an **pendant vertex**
- v is an **odd vertex** if $\deg(v)$ is odd.
 v is an **even vertex** if $\deg(v)$ is even.

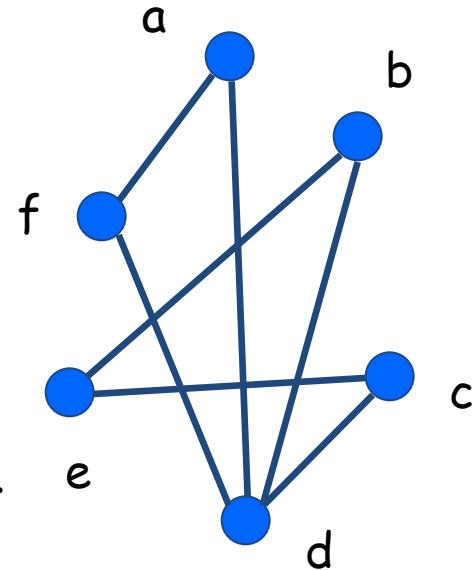


Vertex Degrees

An edge uv is **incident** on the vertex u and the vertex v .

The **neighbour set** $N(v)$ of a vertex v is the set of vertices adjacent to it.

e.g. $N(a) = \{d, f\}$, $N(d) = \{a, b, c, f\}$, $N(e) = \{b, c\}$.



degree of a vertex = # of **incident** edges

e.g. $\deg(d) = 4$, $\deg(a) = \deg(b) = \deg(c) = \deg(e) = \deg(f) = 2$.

the degree of a vertex v = the number of neighbours of v ?

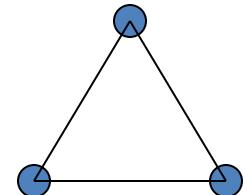
For multigraphs, **NO**.

For simple graphs, **YES**.

Degree Sequence

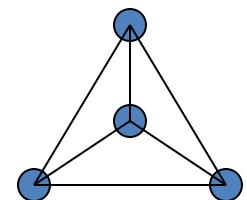
Is there a graph with degree sequence $(2,2,2)$?

YES.



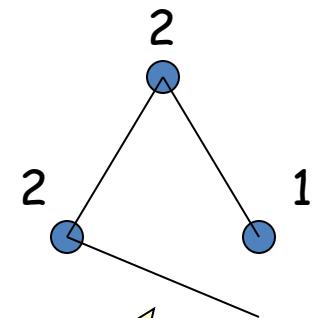
Is there a graph with degree sequence $(3,3,3,3)$?

YES.



Is there a graph with degree sequence $(2,2,1)$?

NO.



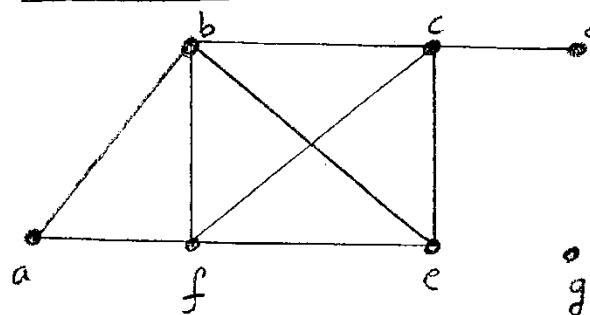
Is there a graph with degree sequence $(2,2,2,2,1)$?

NO.

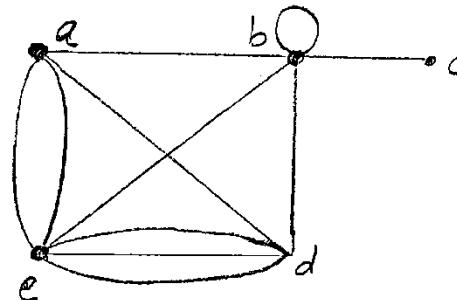
What's wrong with these sequences?

Where to go?

Example:



G



H

What are the degrees of the vertices in the graphs G and H?

The *degree of a vertex in an undirected graph* is the number of edges incident with it, except that a loop at a vertex contributes twice to the degree of that vertex. The degree of the vertex v is denoted by $\deg(v)$.

Solution: In G, $\deg(a)=2$, $\deg(b)=\deg(c)=\deg(f)=4$,
 $\deg(d)=1$, $\deg(e)=3$, $\deg(g)=0$.

In H, $\deg(a)=4$, $\deg(b)=\deg(c)=6$, $\deg(d)=1$,
and $\deg(e)=5$.

Handshaking Lemma

For any graph, sum of degrees = twice # edges

Lemma.

$$2|E| = \sum_{v \in V} \deg(v)$$

Corollary.

1. Sum of degree is an even number.
2. Number of odd degree vertices is even.

Examples.

$2+2+1 = \text{odd}$, so impossible.

$2+2+2+2+1 = \text{odd}$, so impossible.

Handshaking Lemma

Lemma.

$$2|E| = \sum_{v \in V} \deg(v)$$

Proof. Each edge contributes 2 to the sum on the right.

Question. Given a degree sequence, if the sum of degree is even, is it true that there is a graph with such a degree sequence?

For simple graphs, **NO**, consider the degree sequence (3,3,3,1).

For multigraphs (with self loops), **YES!** (easy by induction)

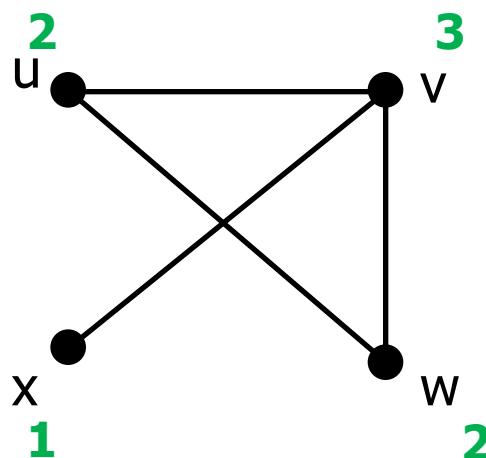
Handshaking theorem

- **Theorem 1.1 (Handshaking theorem)**

Let G be a graph, then

$$\sum_{v \in V(G)} \deg(v) = |E(G)| \times 2$$

Example:



$$\sum_{v \in V(G)} \deg(v) = 8$$

$$|E(G)| = 4$$

Handshaking theorem

Corollary 1.1

Every graph contains an even number of odd vertices.

Proof: If the number of vertices with odd degree is odd, then the degree sum must be odd. →←

Example: How many edges are there in a graph with 10 vertices each of degree 6?

Example: How many edges are there in a graph with 10 vertices each of degree 6?

Solution:

$$\text{Sum of degrees of vertices} = 6 \cdot 10 = 60$$

$$2e = 60 \Rightarrow e = \frac{60}{2} = 30 \text{ edges.}$$

Example: A certain graph G has order 14 and size 27.

The degree of each vertex of G is 3, 4 or 5.

There are six vertices of degree 4.

How many vertices of G have degree 3 and how many have degree 5 ?

Solution: Let x be the number of vertices of G having degree 3.

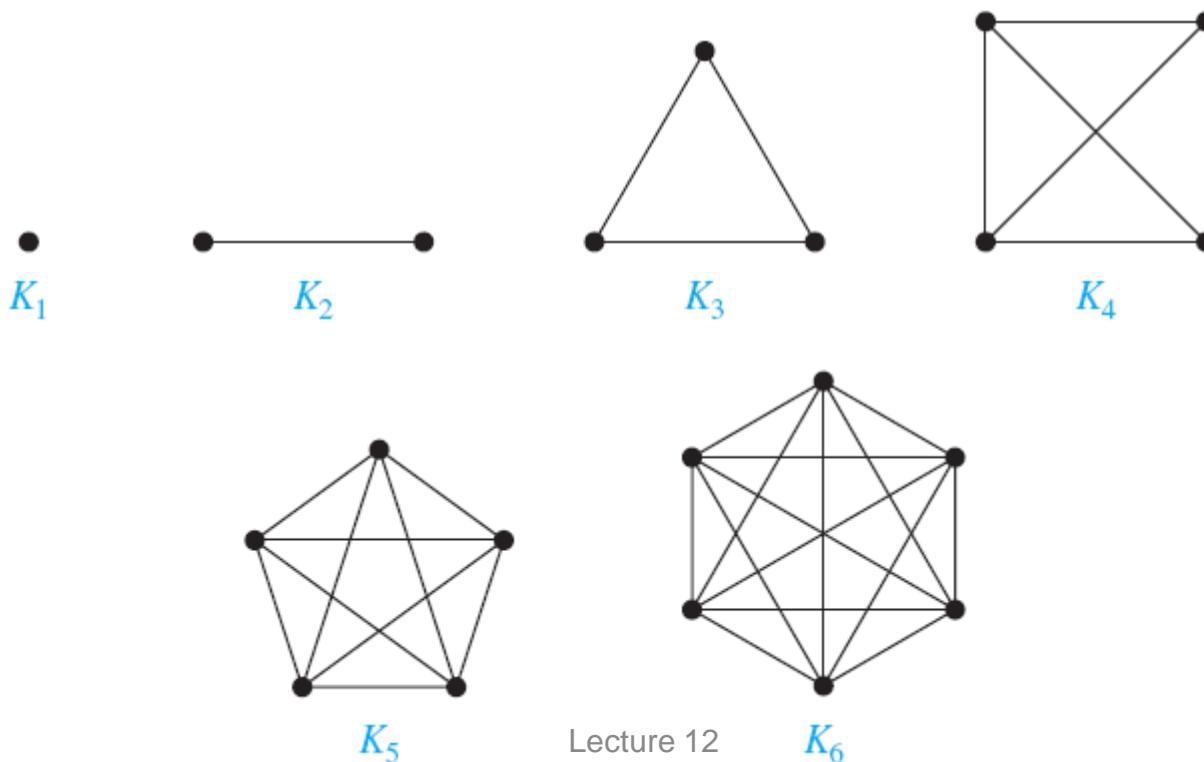
$14 - 6 = 8$ vertices have degree 3 or 5. So there are $8 - x$ vertices of degree 5.

Then we have $3 \cdot x + 4 \cdot 6 + 5 \cdot (8 - x) = 2 \cdot 27$

Hence $x = 5$, $8 - x = 3$

Some Special Simple Graphs

Complete Graphs A **complete graph on n vertices**, denoted by K_n , is a simple graph that contains exactly one edge between each pair of distinct vertices. The graphs K_n , for $n = 1, 2, 3, 4, 5, 6$, are displayed in Figure 3. A simple graph for which there is at least one pair of distinct vertex not connected by an edge is called **noncomplete**. 



Cycles A **cycle** C_n , $n \geq 3$, consists of n vertices v_1, v_2, \dots, v_n and edges $\{v_1, v_2\}$, $\{v_2, v_3\}, \dots, \{v_{n-1}, v_n\}$, and $\{v_n, v_1\}$. The cycles C_3 , C_4 , C_5 , and C_6 are displayed in Figure 4. 

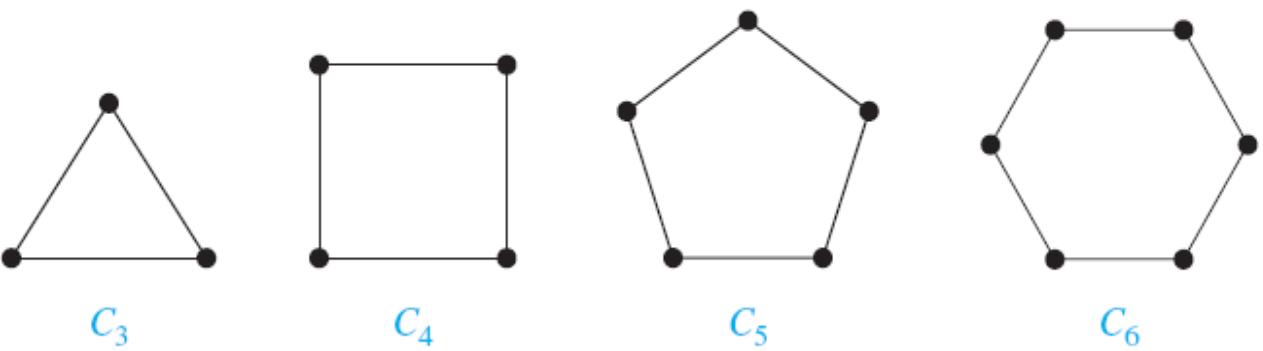


FIGURE 4 The Cycles C_3 , C_4 , C_5 , and C_6 .

Wheels We obtain a **wheel** W_n when we add an additional vertex to a cycle C_n , for $n \geq 3$, and connect this new vertex to each of the n vertices in C_n , by new edges. The wheels W_3 , W_4 , W_5 , and W_6 are displayed in Figure 5.

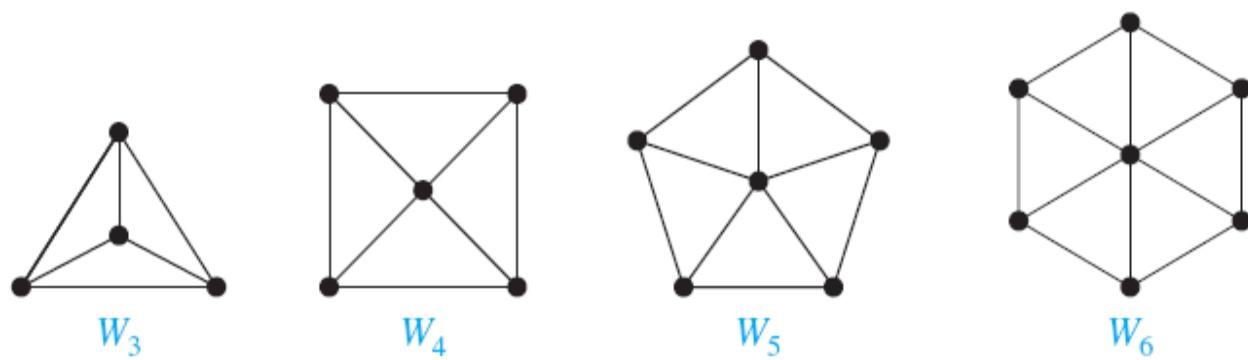


FIGURE 5 The Wheels W_3 , W_4 , W_5 , and W_6 .

n -Cubes An **n -dimensional hypercube**, or **n -cube**, denoted by Q_n , is a graph that has vertices representing the 2^n bit strings of length n . Two vertices are adjacent if and only if the bit strings that they represent differ in exactly one bit position. We display Q_1 , Q_2 , and Q_3 in Figure 6.

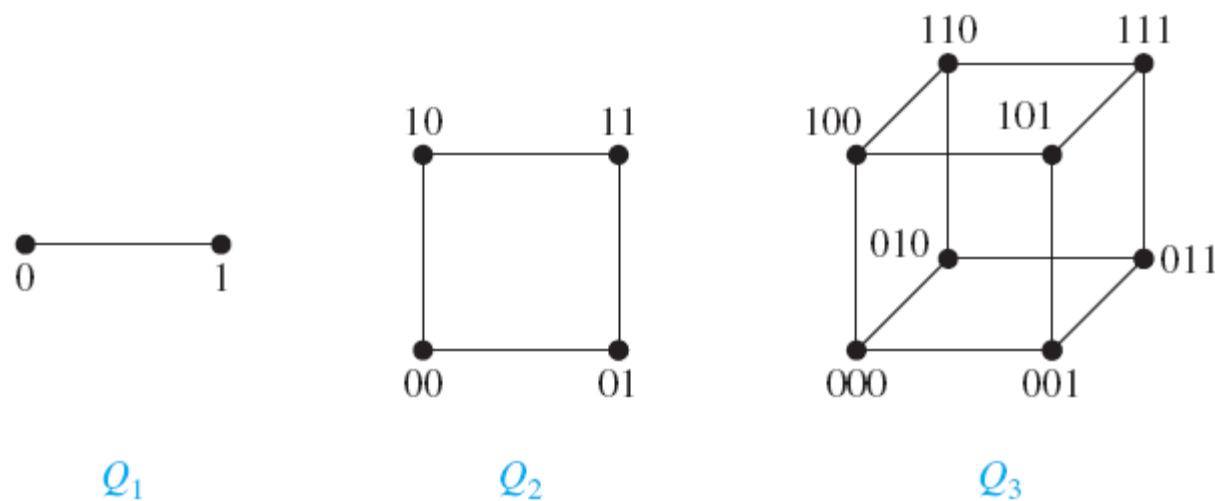


FIGURE 6 The n -cube Q_n , $n = 1, 2, 3$.

Note that you can construct the $(n + 1)$ -cube Q_{n+1} from the n -cube Q_n by making two copies of Q_n , prefacing the labels on the vertices with a 0 in one copy of Q_n and with a 1 in the other copy of Q_n , and adding edges connecting two vertices that have labels differing only in the first bit. In Figure 6, Q_3 is constructed from Q_2 by drawing two copies of Q_2 as the top and bottom faces of Q_3 , adding 0 at the beginning of the label of each vertex in the bottom face and 1 at the beginning of the label of each vertex in the top face. (Here, by *face* we mean a face of a cube in three-dimensional space. Think of drawing the graph Q_3 in three-dimensional space with copies of Q_2 as the top and bottom faces of a cube and then drawing the projection of the resulting depiction in the plane.)

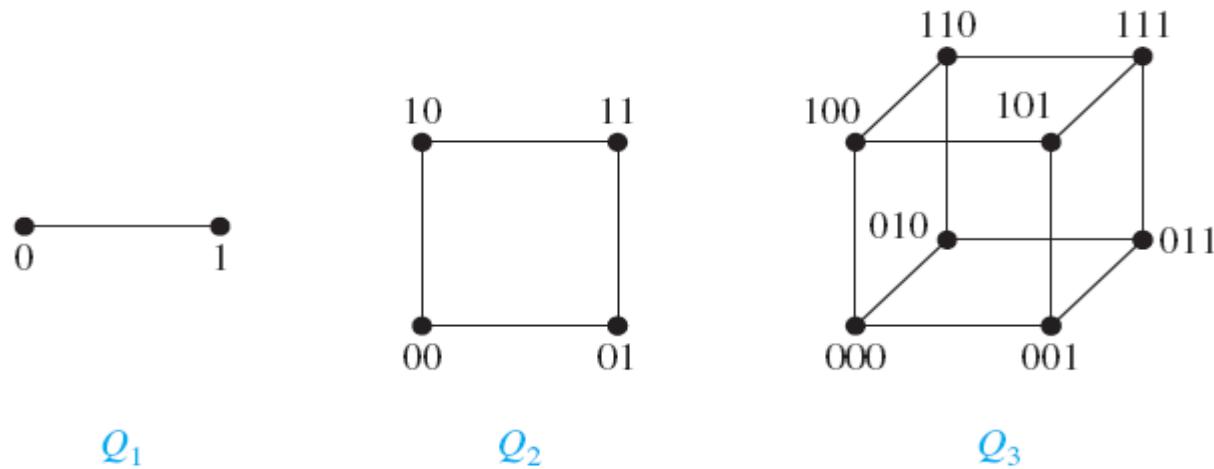


FIGURE 6 The n -cube Q_n , $n = 1, 2, 3$.

Bipartite Graphs

Sometimes a graph has the property that its vertex set can be divided into two disjoint subsets such that each edge connects a vertex in one of these subsets to a vertex in the other subset. For example, consider the graph representing marriages between men and women in a village, where each person is represented by a vertex and a marriage is represented by an edge. In this graph, each edge connects a vertex in the subset of vertices representing males and a vertex in the subset of vertices representing females.

DEFINITION

A simple graph G is called *bipartite* if its vertex set V can be partitioned into two disjoint sets V_1 and V_2 such that every edge in the graph connects a vertex in V_1 and a vertex in V_2 (so that no edge in G connects either two vertices in V_1 or two vertices in V_2). When this condition holds, we call the pair (V_1, V_2) a *bipartition* of the vertex set V of G .

EXAMPLE

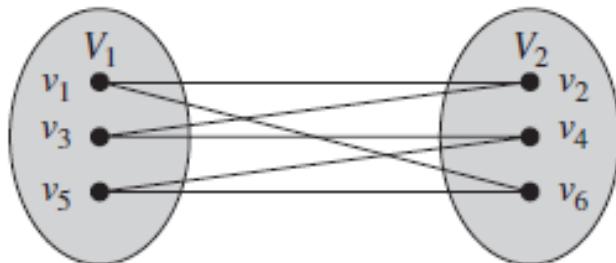


FIGURE 7 Showing That C_6 Is Bipartite.

C_6 is bipartite, as shown in Figure 7, because its vertex set can be partitioned into the two sets $V_1 = \{v_1, v_3, v_5\}$ and $V_2 = \{v_2, v_4, v_6\}$, and every edge of C_6 connects a vertex in V_1 and a vertex in V_2 . ◀

K_3 is not bipartite. To verify this, note that if we divide the vertex set of K_3 into two disjoint sets, one of the two sets must contain two vertices. If the graph were bipartite, these two vertices could not be connected by an edge, but in K_3 each vertex is connected to every other vertex by an edge. ◀

EXAMPLE 11 Are the graphs G and H displayed in Figure 8 bipartite?

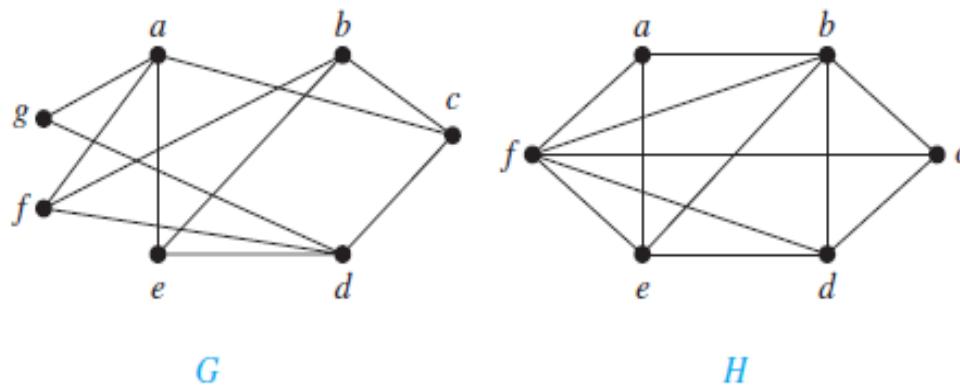


FIGURE 8 The Undirected Graphs G and H .

Solution: Graph G is bipartite because its vertex set is the union of two disjoint sets, $\{a, b, d\}$ and $\{c, e, f, g\}$, and each edge connects a vertex in one of these subsets to a vertex in the other subset. (Note that for G to be bipartite it is not necessary that every vertex in $\{a, b, d\}$ be adjacent to every vertex in $\{c, e, f, g\}$. For instance, b and g are not adjacent.)

Graph H is not bipartite because its vertex set cannot be partitioned into two subsets so that edges do not connect two vertices from the same subset. (The reader should verify this by considering the vertices a , b , and f .) 

Theorem 4 provides a useful criterion for determining whether a graph is bipartite.

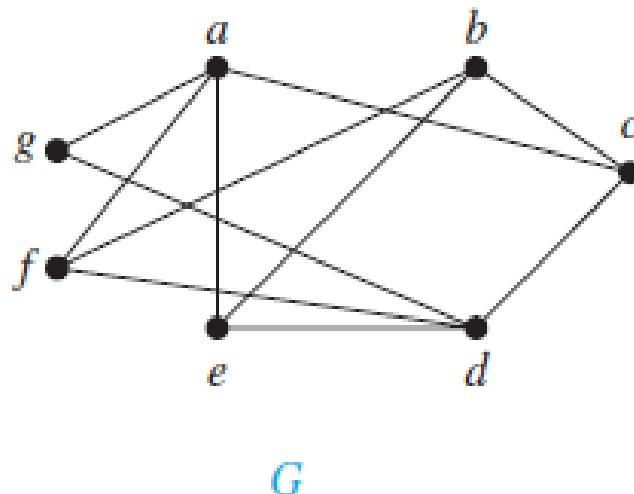
THEOREM 4

A simple graph is bipartite if and only if it is possible to assign one of two different colors to each vertex of the graph so that no two adjacent vertices are assigned the same color.

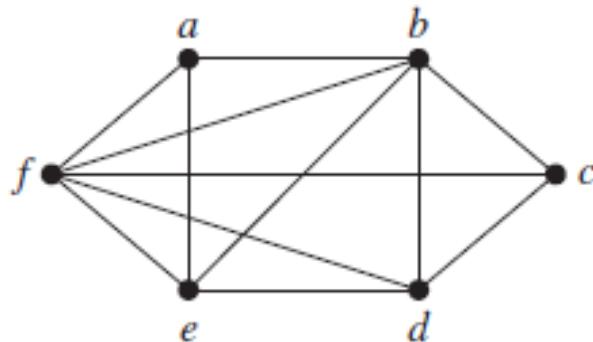
Proof: First, suppose that $G = (V, E)$ is a bipartite simple graph. Then $V = V_1 \cup V_2$, where V_1 and V_2 are disjoint sets and every edge in E connects a vertex in V_1 and a vertex in V_2 . If we assign one color to each vertex in V_1 and a second color to each vertex in V_2 , then no two adjacent vertices are assigned the same color.

Now suppose that it is possible to assign colors to the vertices of the graph using just two colors so that no two adjacent vertices are assigned the same color. Let V_1 be the set of vertices assigned one color and V_2 be the set of vertices assigned the other color. Then, V_1 and V_2 are disjoint and $V = V_1 \cup V_2$. Furthermore, every edge connects a vertex in V_1 and a vertex in V_2 because no two adjacent vertices are either both in V_1 or both in V_2 . Consequently, G is bipartite. 

EXAMPLE 12 Use Theorem 4 to determine whether the graphs in Example 11 are bipartite.



Solution: We first consider the graph G . We will try to assign one of two colors, say red and blue, to each vertex in G so that no edge in G connects a red vertex and a blue vertex. Without loss of generality we begin by arbitrarily assigning red to a . Then, we must assign blue to c, e, f , and g , because each of these vertices is adjacent to a . To avoid having an edge with two blue endpoints, we must assign red to all the vertices adjacent to either c, e, f , or g . This means that we must assign red to both b and d (and means that a must be assigned red, which it already has been). We have now assigned colors to all vertices, with a, b , and d red and c, e, f , and g blue. Checking all edges, we see that every edge connects a red vertex and a blue vertex. Hence, by Theorem 4 the graph G is bipartite.



H

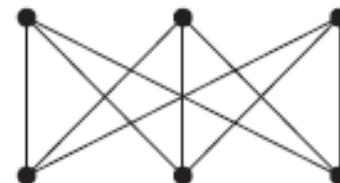
Next, we will try to assign either red or blue to each vertex in H so that no edge in H connects a red vertex and a blue vertex. Without loss of generality we arbitrarily assign red to a . Then, we must assign blue to b, e , and f , because each is adjacent to a . But this is not possible because e and f are adjacent, so both cannot be assigned blue. This argument shows that we cannot assign one of two colors to each of the vertices of H so that no adjacent vertices are assigned the same color. It follows by Theorem 4 that H is not bipartite. \blacktriangleleft

Theorem 4 is an example of a result in the part of graph theory known as graph colorings. Graph colorings is an important part of graph theory with important applications. We will study

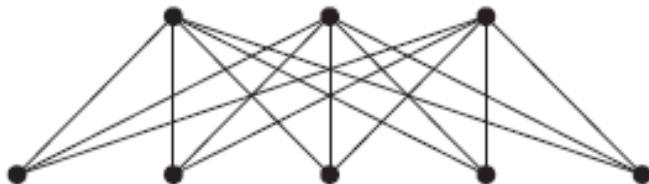
Complete Bipartite Graphs A complete bipartite graph $K_{m,n}$ is a graph that has its vertex set partitioned into two subsets of m and n vertices, respectively with an edge between two vertices if and only if one vertex is in the first subset and the other vertex is in the second subset. The complete bipartite graphs $K_{2,3}$, $K_{3,3}$, $K_{3,5}$, and $K_{2,6}$ are displayed in Figure 9. 



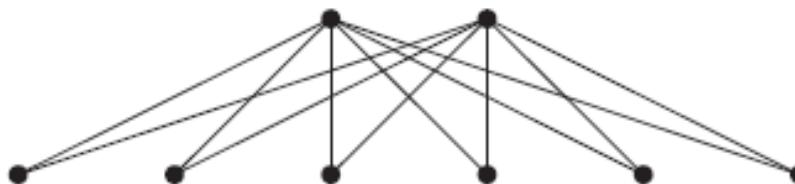
$K_{2,3}$



$K_{3,3}$



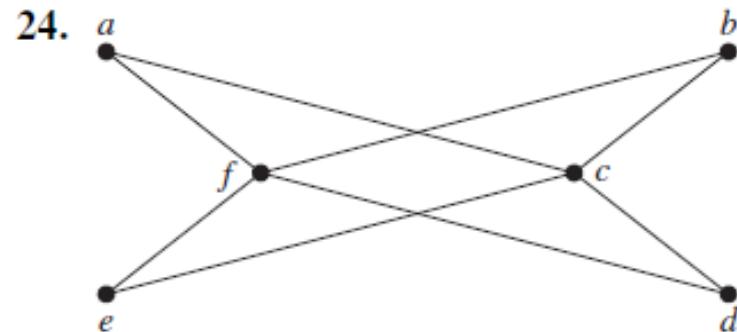
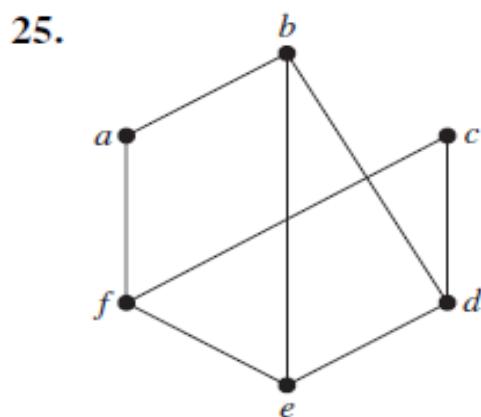
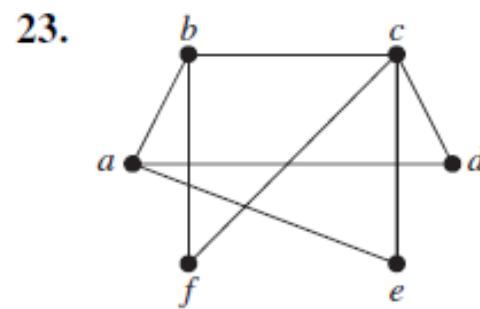
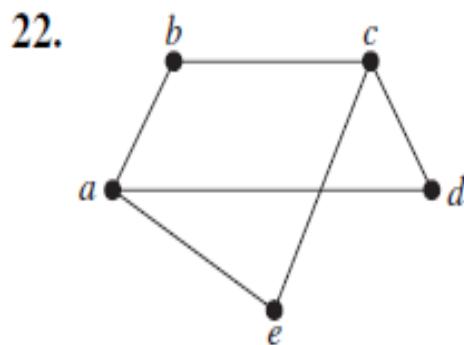
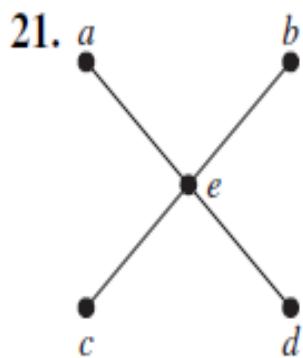
$K_{3,5}$



$K_{2,6}$

FIGURE 9 Some Complete Bipartite Graphs.

In Exercises 21–25 determine whether the graph is bipartite. You may find it useful to apply Theorem 4 and answer the question by determining whether it is possible to assign either red or blue to each vertex so that no two adjacent vertices are assigned the same color.



Exercises

For which values of n are these graphs bipartite?

- a) K_n
- b) C_n
- c) W_n
- d) Q_n

- a) By the definition given in the text, K_1 does not have enough vertices to be bipartite. Clearly K_2 is bipartite. There is a triangle in K_n for $n > 2$, so those complete graphs are not bipartite.
- b) First we need $n \geq 3$ for C_n to be defined. If n is even, then C_n is bipartite, since we can take one part to be every other vertex. If n is odd, then C_n is not bipartite.
- c) Every wheel contains triangles, so no W_n is bipartite.
- d) Q_n is bipartite for all $n \geq 1$, since we can divide the vertices into these two classes: those bit strings with an odd number of 1's, and those bit strings with an even number of 1's.

Example How many vertices and how many edges do these graphs have?

a) K_n
d) $K_{m,n}$

b) C_n
e) Q_n

c) W_n

a) n vertices, $\frac{n(n - 1)}{2}$ edges

b) n vertices, n edges

c) $n + 1$ vertices, $2n$ edges

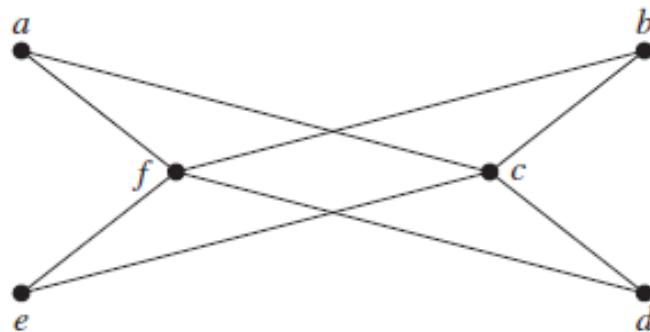
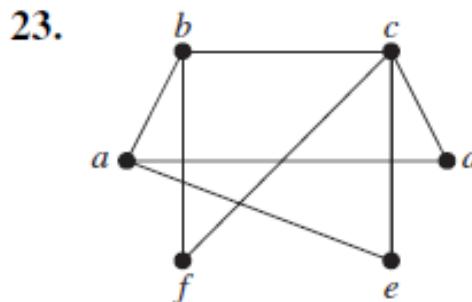
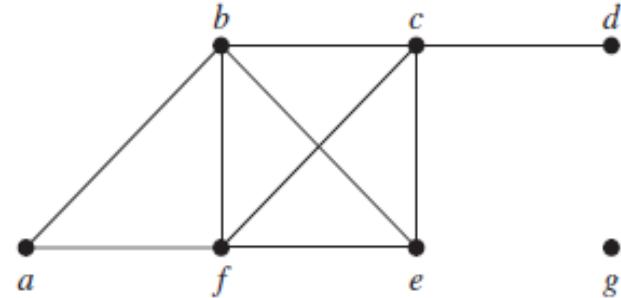
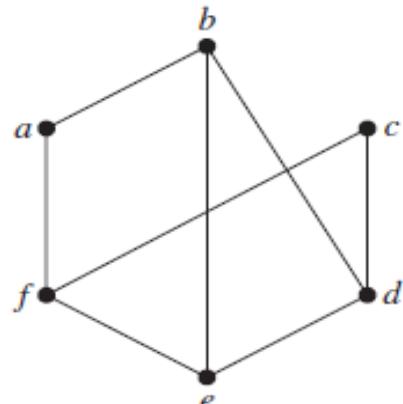
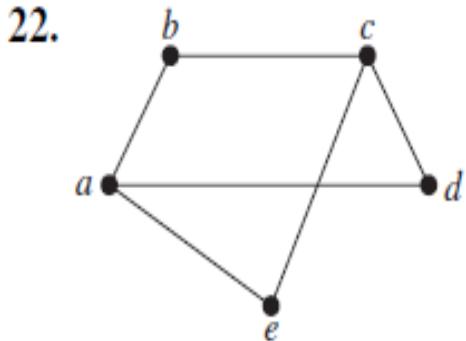
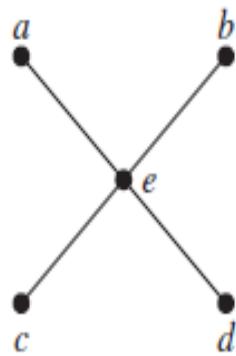
d) $m + n$ vertices, mn edges

e) 2^n vertices, $n2^{n-1}$ edges

DEFINITION

The **degree sequence** of a graph is the sequence of the degrees of the vertices of the graph in nonincreasing order. For example, the degree sequence of the graph G in Example 1 is $4, 4, 4, 3, 2, 1, 0$.

Find the degree sequences for each of the graphs in Exercises 21–25.



Example

Find the degree sequence of each of the following graphs.

a) K_4

d) $K_{2,3}$

b) C_4

e) Q_3

c) W_4

a) 3, 3, 3, 3

Example

Find the degree sequence of each of the following graphs.

a) K_4

d) $K_{2,3}$

b) C_4

e) Q_3

c) W_4

a) 3, 3, 3, 3 b) 2, 2, 2, 2

Example

Find the degree sequence of each of the following graphs.

a) K_4

d) $K_{2,3}$

b) C_4

e) Q_3

c) W_4

a) 3, 3, 3, 3 b) 2, 2, 2, 2 c) 4, 3, 3, 3, 3

Example

Find the degree sequence of each of the following graphs.

a) K_4

d) $K_{2,3}$

b) C_4

e) Q_3

c) W_4

- a) 3, 3, 3, 3 b) 2, 2, 2, 2 c) 4, 3, 3, 3, 3 d) 3, 3, 2, 2, 2

Example

Find the degree sequence of each of the following graphs.

a) K_4

d) $K_{2,3}$

b) C_4

e) Q_3

c) W_4

- a) 3, 3, 3, 3 b) 2, 2, 2, 2 c) 4, 3, 3, 3, 3 d) 3, 3, 2, 2, 2 e) 3, 3, 3, 3, 3, 3, 3, 3

Example Find the degree sequence of each of the following graphs.

- a) K_4 b) C_4 c) W_4
d) $K_{2,3}$ e) Q_3
- a) 3, 3, 3, 3 b) 2, 2, 2, 2 c) 4, 3, 3, 3, 3 d) 3, 3, 2, 2, 2 e) 3, 3, 3, 3, 3, 3, 3

What is the degree sequence of the bipartite graph $K_{m,n}$ where m and n are positive integers? Explain your answer.

What is the degree sequence of K_n , where n is a positive integer? Explain your answer. $n-1, n-1, \dots, n-1$ (n terms)

How many edges does a graph have if its degree sequence is 4, 3, 3, 2, 2? Draw such a graph.

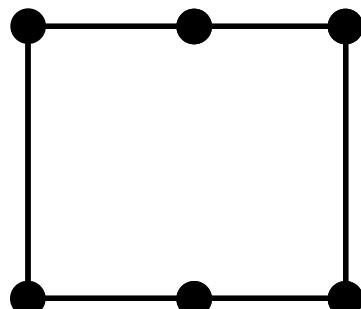
Regular graph

Definition:

A graph G is **r-regular** if every vertex of G has degree r .

A graph G is **regular** if it's **r-regular** for some r .

Example:



2-regular

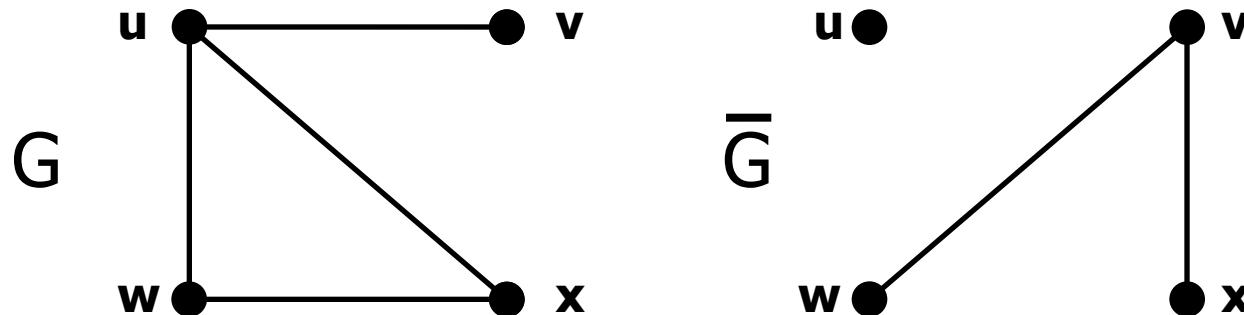
Note.

There is no 1-regular graph or 3-regular graph of order 5.
(by Corollary 1.1)

Complement

Definition.

The **complement** \bar{G} of a graph G is a graph with $V(G) = V(\bar{G})$, and $uv \in E(G)$ iff $uv \notin E(\bar{G})$.



Exercise .

Every vertex of a graph G of order 14 and size 25 has degree 3 or 5.

How many vertices of degree 3 does G have?

sol. Suppose there are x vertices of degree 3, then there are $14-x$ vertices of degree 5.

$$|E(G)| = 25 \Rightarrow \text{degree sum} = 50$$

$$3x + 5(14-x) = 50$$

$$\Rightarrow x = 10$$

Exercise 10.

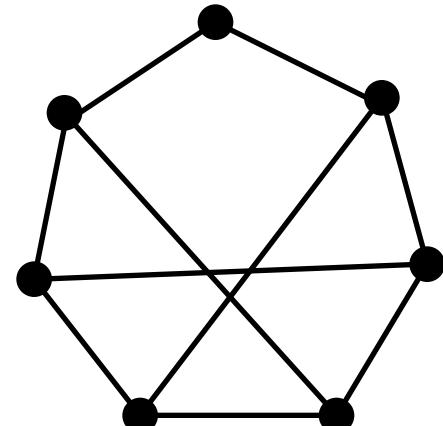
A graph G of order 7 and size 10 has six vertices of degree a and one of degree b . What is b ?

sol. $6a + b = 20$

- | | |
|--------------------|------------------|
| $(a, b) = (0, 20)$ | (\times) |
| $(1, 14)$ | (\times) |
| $(2, 8)$ | (\times) |
| $(3, 2)$ | (\checkmark) |

$\therefore a=3, b=2.$

Try to draw the graph



The **complementary graph** \overline{G} of a simple graph G has the same vertices as G . Two vertices are adjacent in \overline{G} if and only if they are not adjacent in G . Describe each of these graphs.

- a)** $\overline{K_n}$ **b)** $\overline{K_{m,n}}$ **c)** $\overline{C_n}$ **d)** $\overline{Q_n}$

- a) The graph with n vertices and no edges
- b) The disjoint union of K_m and K_n
- c) The graph with vertices $\{v_1, \dots, v_n\}$ with an edge between v_i and v_j unless $i \equiv j \pm 1 \pmod n$
- d) The graph whose vertices are represented by bit strings of length n with an edge between two vertices if the associated bit strings differ in more than one bit

Example: If G is a simple graph with 15 edges and \overline{G} has 13 edges, how many vertices does G have?

Exercises

1. If the simple graph G has v vertices and e edges, how many edges does \overline{G} have?
 2. If the degree sequence of the simple graph G is 4, 3, 3, 2, 2, what is the degree sequence of \overline{G} ?
 3. If the degree sequence of the simple graph G is d_1, d_2, \dots, d_n , what is the degree sequence of \overline{G} ?
-
1. $v(v - 1)/2 - e$
 3. $n - 1 - d_n, n - 1 - d_{n-1}, \dots, n - 1 - d_2, n - 1 - d_1$

A simple graph is called **regular** if every vertex of this graph has the same degree. A regular graph is called *n*-**regular** if every vertex in this graph has degree *n*.

Example:

- For which values of *n* are these graphs regular?
 - a) K_n
 - b) C_n
 - c) W_n
 - d) Q_n
- For which values of *m* and *n* is $K_{m,n}$ regular?
- How many vertices does a regular graph of degree four with 10 edges have?
 - a) For all $n \geq 1$
 - b) For all $n \geq 3$
 - c) For $n = 3$
 - d) For all $n \geq 0$

New Graphs from Old

Sometimes we need only part of a graph to solve a problem. For instance, we may care only about the part of a large computer network that involves the computer centers in New York, Denver, Detroit, and Atlanta. Then we can ignore the other computer centers and all telephone lines not linking two of these specific four computer centers. In the graph model for the large network, we can remove the vertices corresponding to the computer centers other than the four of interest, and we can remove all edges incident with a vertex that was removed. When edges and vertices are removed from a graph, without removing endpoints of any remaining edges, a smaller graph is obtained. Such a graph is called a **subgraph** of the original graph.

A *subgraph* of a graph $G = (V, E)$ is a graph $H = (W, F)$, where $W \subseteq V$ and $F \subseteq E$. A subgraph H of G is a *proper subgraph* of G if $H \neq G$.

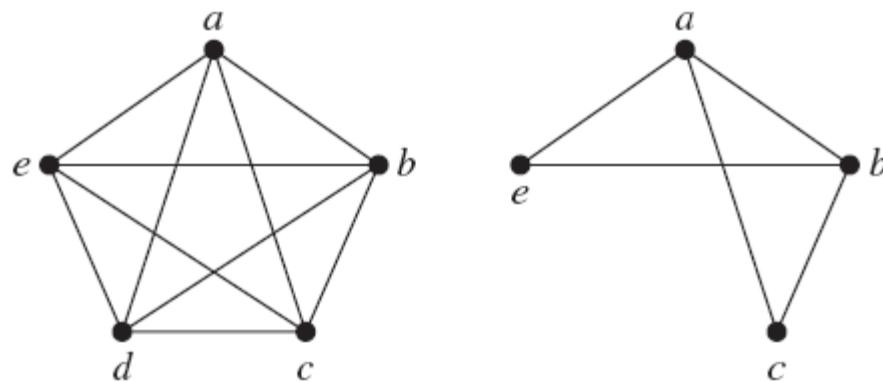
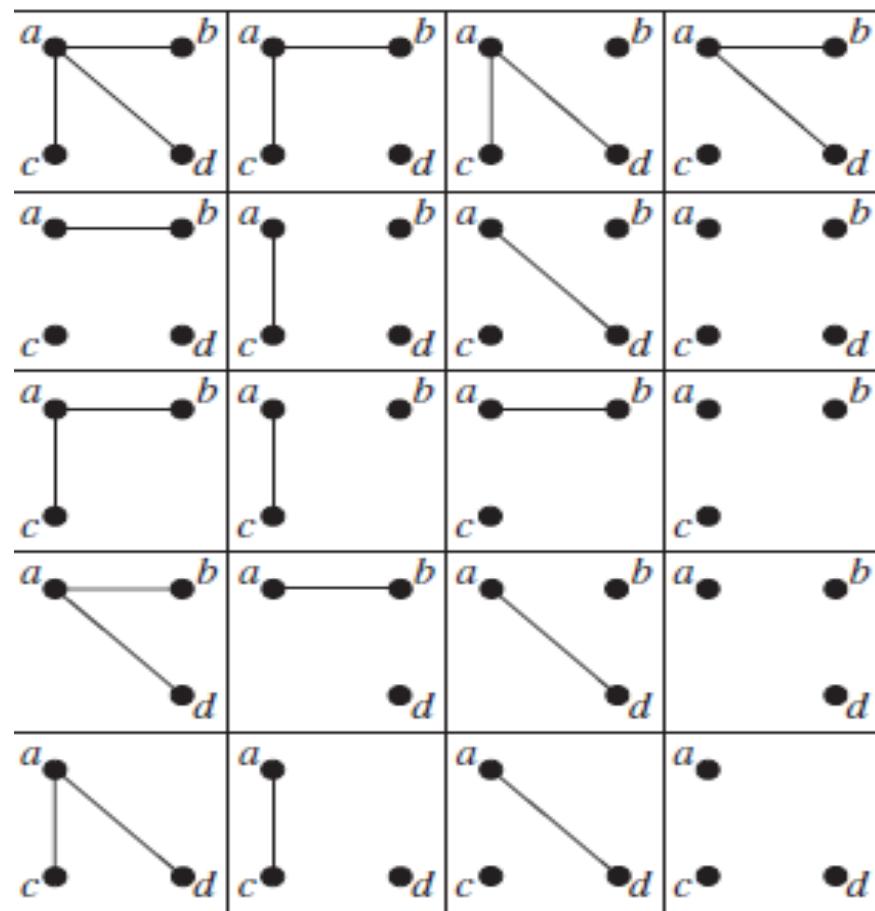
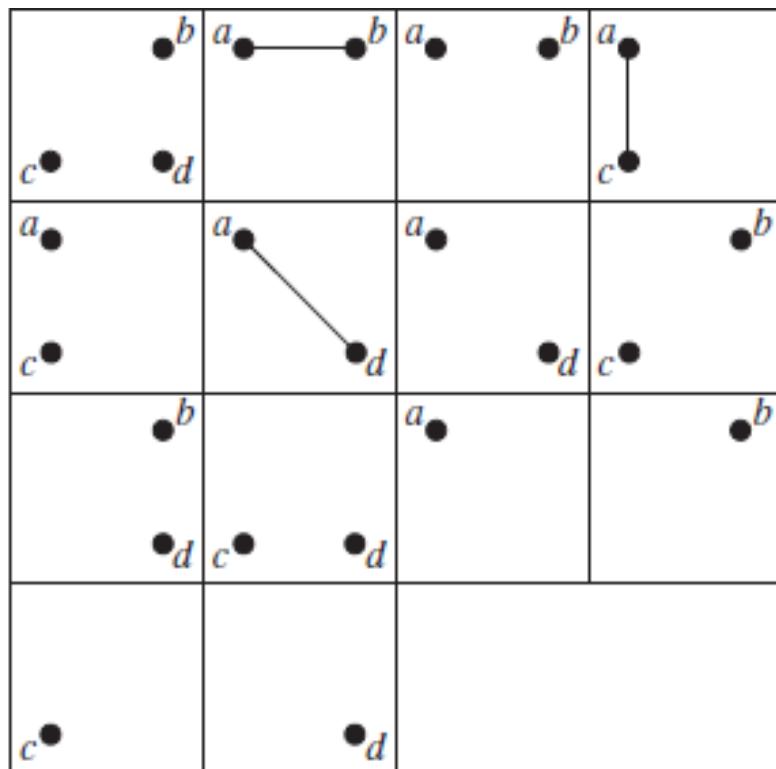
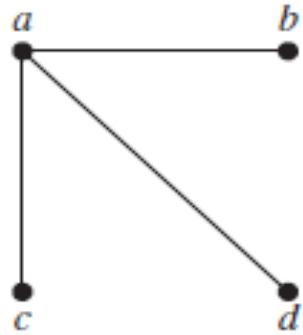


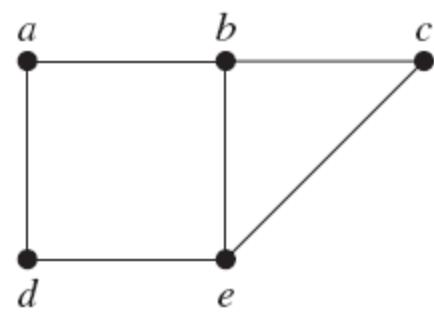
FIGURE 15 A Subgraph of K_5 .

Example: Draw all subgraphs of this graph.



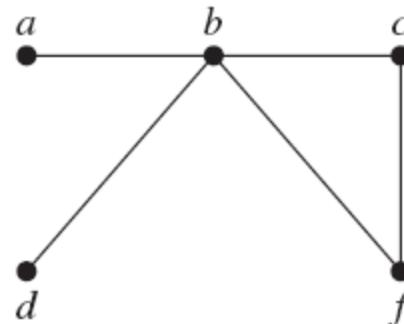
GRAPH UNIONS Two or more graphs can be combined in various ways. The new graph that contains all the vertices and edges of these graphs is called the **union** of the graphs. We will give a more formal definition for the union of two simple graphs.

The *union* of two simple graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is the simple graph with vertex set $V_1 \cup V_2$ and edge set $E_1 \cup E_2$. The union of G_1 and G_2 is denoted by $G_1 \cup G_2$.



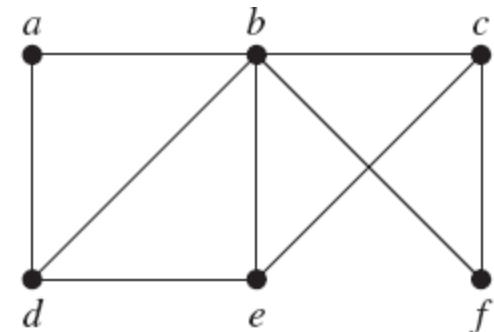
G_1

(a)



G_2

(b)

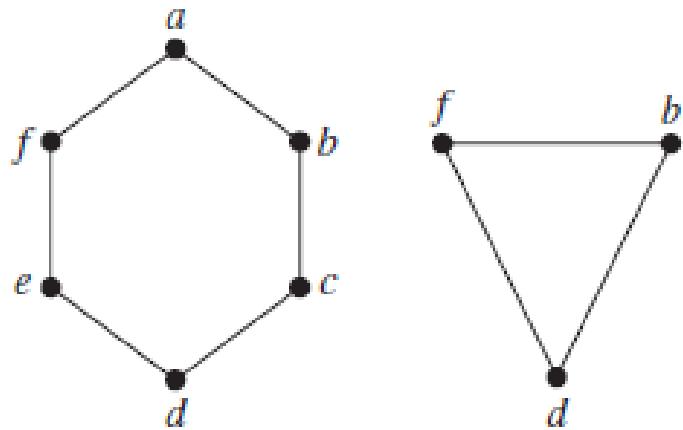


$G_1 \cup G_2$

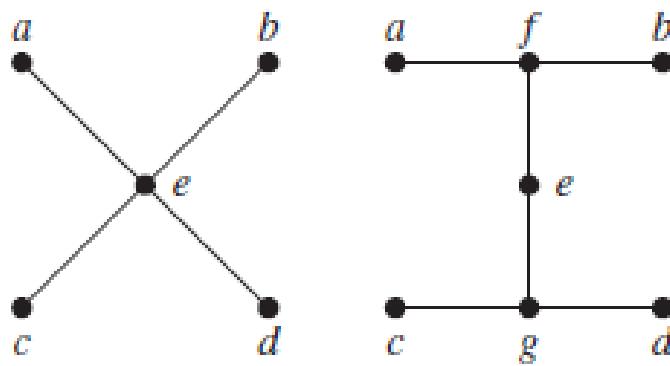
FIGURE 16 (a) The Simple Graphs G_1 and G_2 ; (b) Their Union $G_1 \cup G_2$.

In Exercises 56–58 find the union of the given pair of simple graphs. (Assume edges with the same endpoints are the same.)

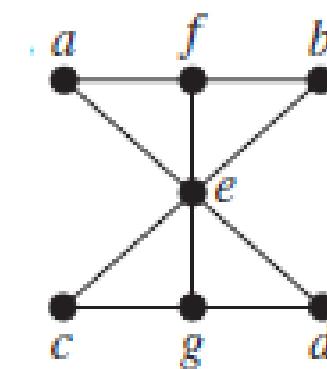
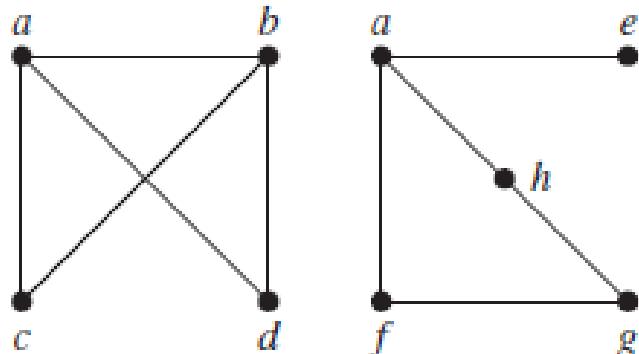
56.



57.



58.



Mat2033 - Discrete Mathematics

Graph Theory and Its Applications

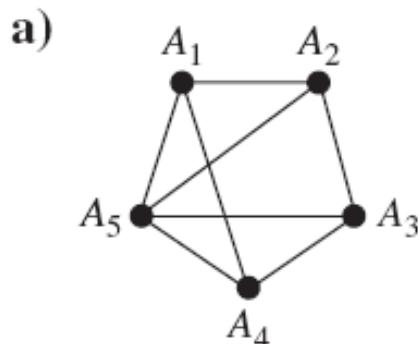
The **intersection graph** of a collection of sets A_1, A_2, \dots, A_n is the graph that has a vertex for each of these sets and has an edge connecting the vertices representing two sets if these sets have a nonempty intersection. Construct the intersection graph of these collections of sets.

a) $A_1 = \{0, 2, 4, 6, 8\}$, $A_2 = \{0, 1, 2, 3, 4\}$,
 $A_3 = \{1, 3, 5, 7, 9\}$, $A_4 = \{5, 6, 7, 8, 9\}$,
 $A_5 = \{0, 1, 8, 9\}$

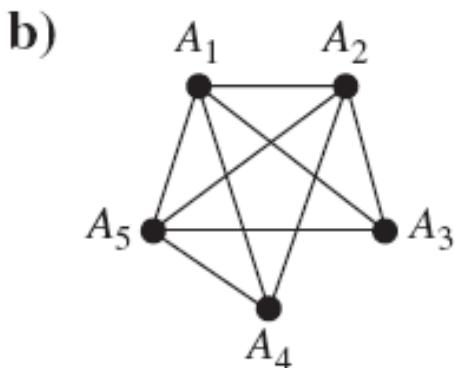
b) $A_1 = \{\dots, -4, -3, -2, -1, 0\}$,
 $A_2 = \{\dots, -2, -1, 0, 1, 2, \dots\}$,
 $A_3 = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}$,
 $A_4 = \{\dots, -5, -3, -1, 1, 3, 5, \dots\}$,
 $A_5 = \{\dots, -6, -3, 0, 3, 6, \dots\}$

c) $A_1 = \{x \mid x < 0\}$,
 $A_2 = \{x \mid -1 < x < 0\}$,
 $A_3 = \{x \mid 0 < x < 1\}$,
 $A_4 = \{x \mid -1 < x < 1\}$,
 $A_5 = \{x \mid x > -1\}$,
 $A_6 = \mathbf{R}$

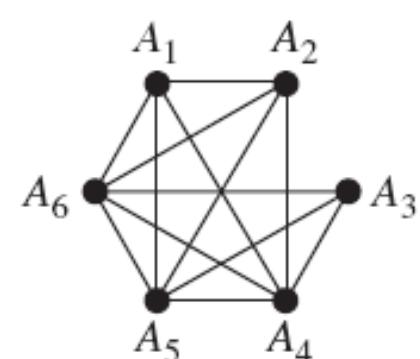
- a) $A_1 = \{0, 2, 4, 6, 8\}$, $A_2 = \{0, 1, 2, 3, 4\}$,
 $A_3 = \{1, 3, 5, 7, 9\}$, $A_4 = \{5, 6, 7, 8, 9\}$,
 $A_5 = \{0, 1, 8, 9\}$



- b) $A_1 = \{\dots, -4, -3, -2, -1, 0\}$,
 $A_2 = \{\dots, -2, -1, 0, 1, 2, \dots\}$,
 $A_3 = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}$,
 $A_4 = \{\dots, -5, -3, -1, 1, 3, 5, \dots\}$,
 $A_5 = \{\dots, -6, -3, 0, 3, 6, \dots\}$



- c) $A_1 = \{x \mid x < 0\}$,
 $A_2 = \{x \mid -1 < x < 0\}$,
 $A_3 = \{x \mid 0 < x < 1\}$,
 $A_4 = \{x \mid -1 < x < 1\}$,
 $A_5 = \{x \mid x > -1\}$,
 $A_6 = \mathbf{R}$



Representing Graphs

One way to represent a graph without multiple edges is to list all the edges of this graph. Another way to represent a graph with no multiple edges is to use **adjacency lists**, which specify the vertices that are adjacent to each vertex of the graph.

Use adjacency lists to describe the simple graph given in Figure 1.

Solution: Table 1 lists those vertices adjacent to each of the vertices of the graph. 

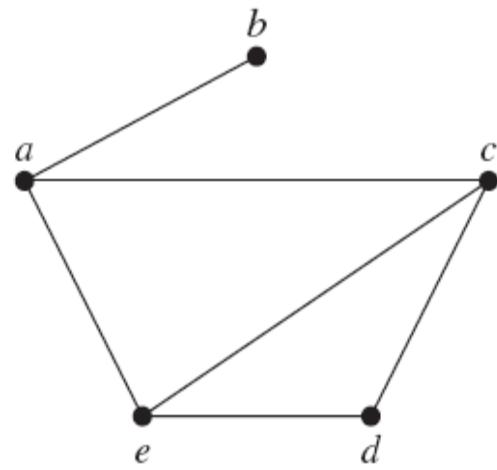


FIGURE 1 A Simple Graph.

TABLE 1 An Adjacency List for a Simple Graph.

<i>Vertex</i>	<i>Adjacent Vertices</i>
<i>a</i>	<i>b, c, e</i>
<i>b</i>	<i>a</i>
<i>c</i>	<i>a, d, e</i>
<i>d</i>	<i>c, e</i>
<i>e</i>	<i>a, c, d</i>

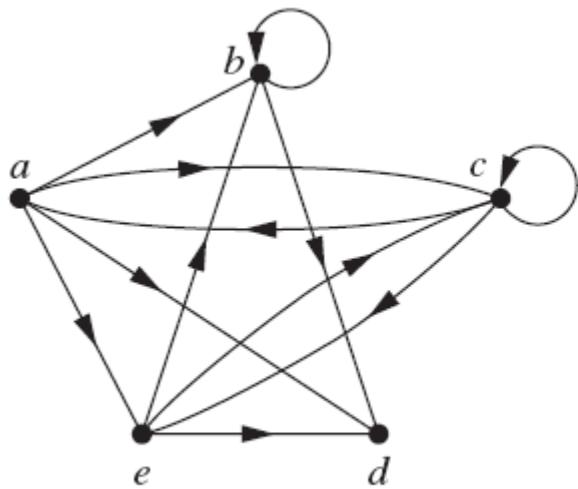


FIGURE 2 A Directed Graph.

TABLE 2 An Adjacency List for a Directed Graph.

<i>Initial Vertex</i>	<i>Terminal Vertices</i>
a	b, c, d, e
b	b, d
c	a, c, e
d	
e	b, c, d

Adjacency Matrices

Carrying out graph algorithms using the representation of graphs by lists of edges, or by adjacency lists, can be cumbersome if there are many edges in the graph. To simplify computation, graphs can be represented using matrices. Two types of matrices commonly used to represent graphs will be presented here. One is based on the adjacency of vertices, and the other is based on incidence of vertices and edges.

Suppose that $G = (V, E)$ is a simple graph where $|V| = n$. Suppose that the vertices of G are listed arbitrarily as v_1, v_2, \dots, v_n . The **adjacency matrix** \mathbf{A} (or \mathbf{A}_G) of G , with respect to this listing of the vertices, is the $n \times n$ zero–one matrix with 1 as its (i, j) th entry when v_i and v_j are adjacent, and 0 as its (i, j) th entry when they are not adjacent. In other words, if its adjacency matrix is $\mathbf{A} = [a_{ij}]$, then

$$a_{ij} = \begin{cases} 1 & \text{if } \{v_i, v_j\} \text{ is an edge of } G, \\ 0 & \text{otherwise.} \end{cases}$$

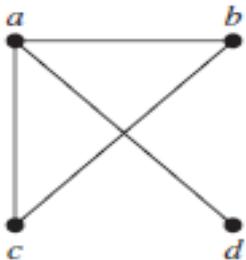


FIGURE 3
Simple Graph.

Use an adjacency matrix to represent the graph shown in Figure 3.

Solution: We order the vertices as a, b, c, d . The matrix representing this graph is

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

Draw a graph with the adjacency matrix

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

with respect to the ordering of vertices a, b, c, d .

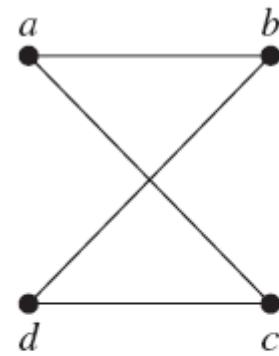


FIGURE 4
**A Graph with the
Given Adjacency
Matrix.**

Adjacency matrices can also be used to represent undirected graphs with loops and with multiple edges. A loop at the vertex v_i is represented by a 1 at the (i, i) th position of the adjacency matrix. When multiple edges connecting the same pair of vertices v_i and v_j , or multiple loops at the same vertex, are present, the adjacency matrix is no longer a zero–one matrix, because the (i, j) th entry of this matrix equals the number of edges that are associated to $\{v_i, v_j\}$. All undirected graphs, including multigraphs and pseudographs, have symmetric adjacency matrices.

Use an adjacency matrix to represent the pseudograph shown in Figure 5.

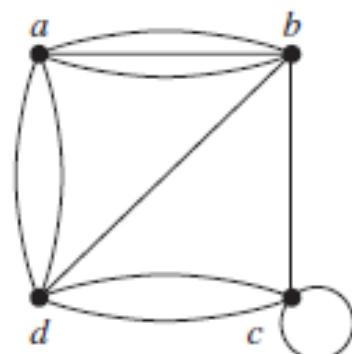
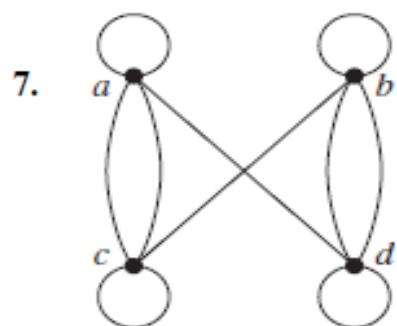
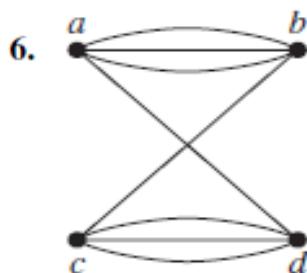
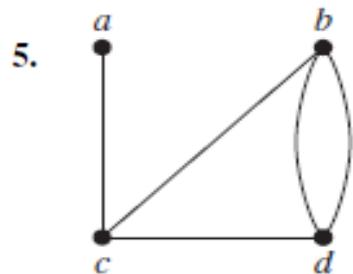
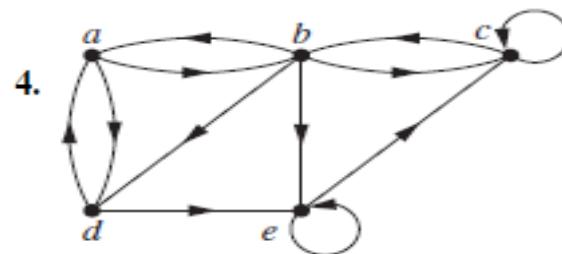
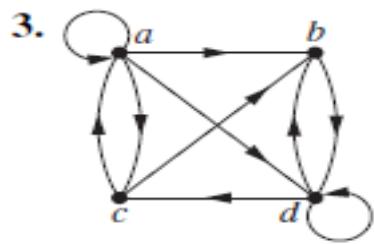
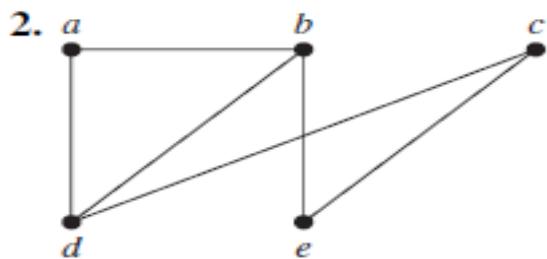
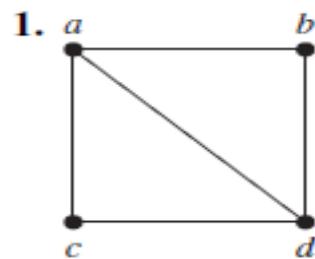


FIGURE 5
A Pseudograph.

Solution: The adjacency matrix using the ordering of vertices a, b, c, d is

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

Example: Represent the following graphs with an adjacency matrix.



Example: Represent each of these graphs with an adjacency matrix.

a) K_4

d) C_4

b) $K_{1,4}$

e) W_4

c) $K_{2,3}$

f) Q_3

a)
$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

b)
$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

c)
$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

d)
$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

e)
$$\begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

f)
$$\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Example: Draw a graph with the given adjacency matrix.

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

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

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

4.
$$\begin{bmatrix} 1 & 3 & 2 \\ 3 & 0 & 4 \\ 2 & 4 & 0 \end{bmatrix}$$

5.
$$\begin{bmatrix} 1 & 2 & 0 & 1 \\ 2 & 0 & 3 & 0 \\ 0 & 3 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

6.
$$\begin{bmatrix} 0 & 1 & 3 & 0 & 4 \\ 1 & 2 & 1 & 3 & 0 \\ 3 & 1 & 1 & 0 & 1 \\ 0 & 3 & 0 & 0 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}$$

Incidence Matrices

Another common way to represent graphs is to use **incidence matrices**. Let $G = (V, E)$ be an undirected graph. Suppose that v_1, v_2, \dots, v_n are the vertices and e_1, e_2, \dots, e_m are the edges of G . Then the incidence matrix with respect to this ordering of V and E is the $n \times m$ matrix $\mathbf{M} = [m_{ij}]$, where

$$m_{ij} = \begin{cases} 1 & \text{when edge } e_j \text{ is incident with } v_i, \\ 0 & \text{otherwise.} \end{cases}$$

EXAMPLE 6 Represent the graph shown in Figure 6 with an incidence matrix.

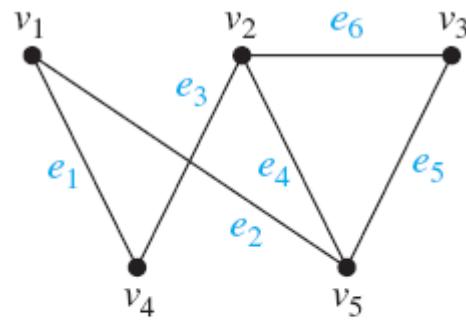


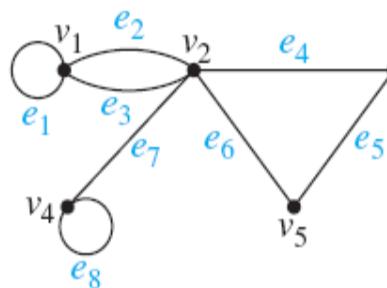
FIGURE 6 An
Undirected
Graph.

Solution: The incidence matrix is

$$\begin{array}{cccccc} & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \\ v_1 & 1 & 1 & 0 & 0 & 0 & 0 \\ v_2 & 0 & 0 & 1 & 1 & 0 & 1 \\ v_3 & 0 & 0 & 0 & 0 & 1 & 1 \\ v_4 & 1 & 0 & 1 & 0 & 0 & 0 \\ v_5 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}.$$

Incidence matrices can also be used to represent multiple edges and loops. Multiple edges are represented in the incidence matrix using columns with identical entries, because these edges are incident with the same pair of vertices. Loops are represented using a column with exactly one entry equal to 1, corresponding to the vertex that is incident with this loop.

EXAMPLE 7 Represent the pseudograph shown in Figure 7 using an incidence matrix.

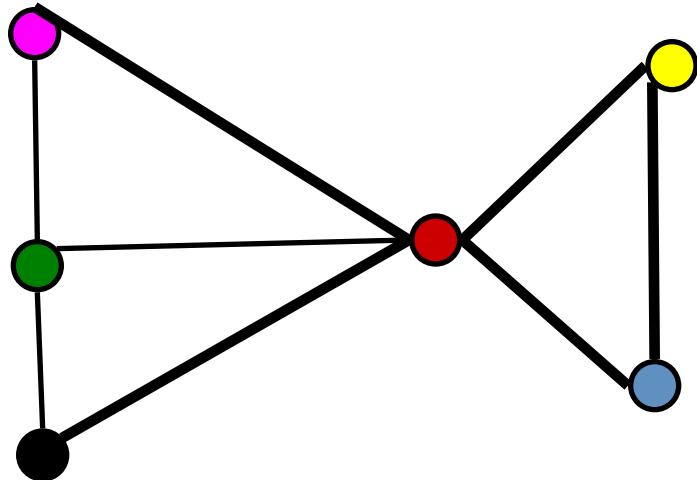


Solution: The incidence matrix for this graph is

$$\begin{array}{c}
 \begin{matrix} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \end{matrix} \\
 \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{matrix} \left[\begin{matrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{matrix} \right].
 \end{array}$$

FIGURE 7
A Pseudograph.

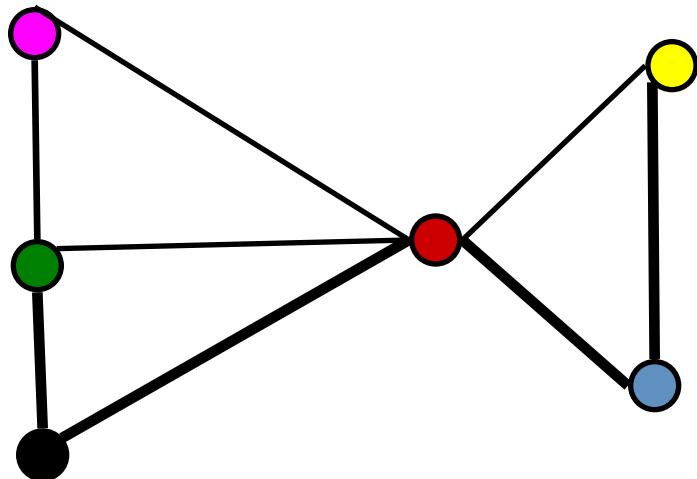
Paths



Path: sequence of *adjacent* vertices

(● ● ● ● ● ●)

Simple Paths



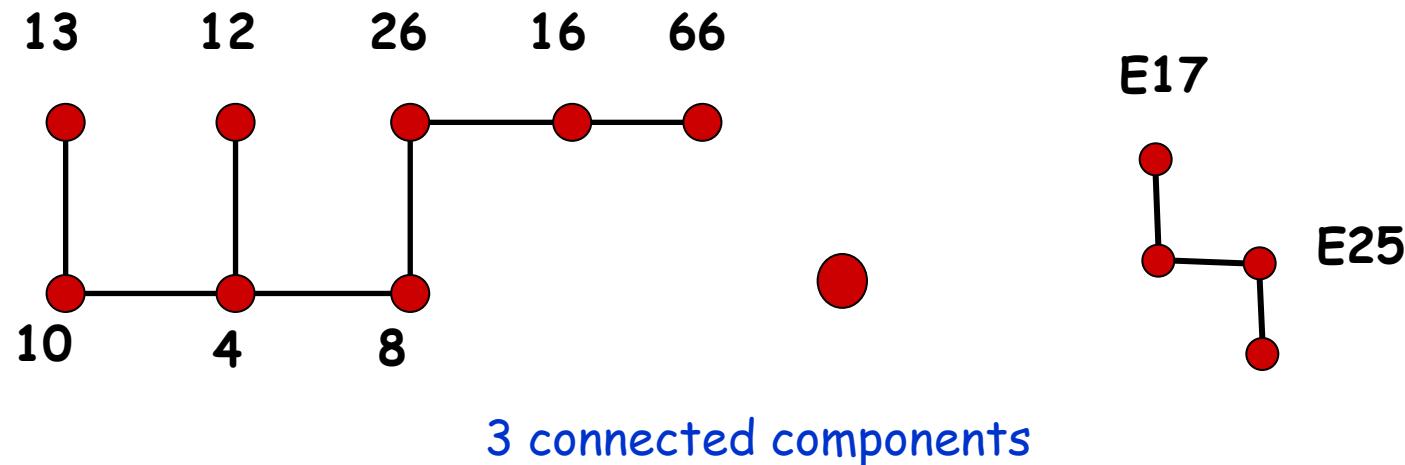
Simple Path: all vertices different

(●●●●●)

Connectedness

- ❖ Vertices v, w are *connected* if and only if
 - there is a path starting at v and ending at w .
- ❖ A *graph* is *connected* iff every pair of vertices are connected.

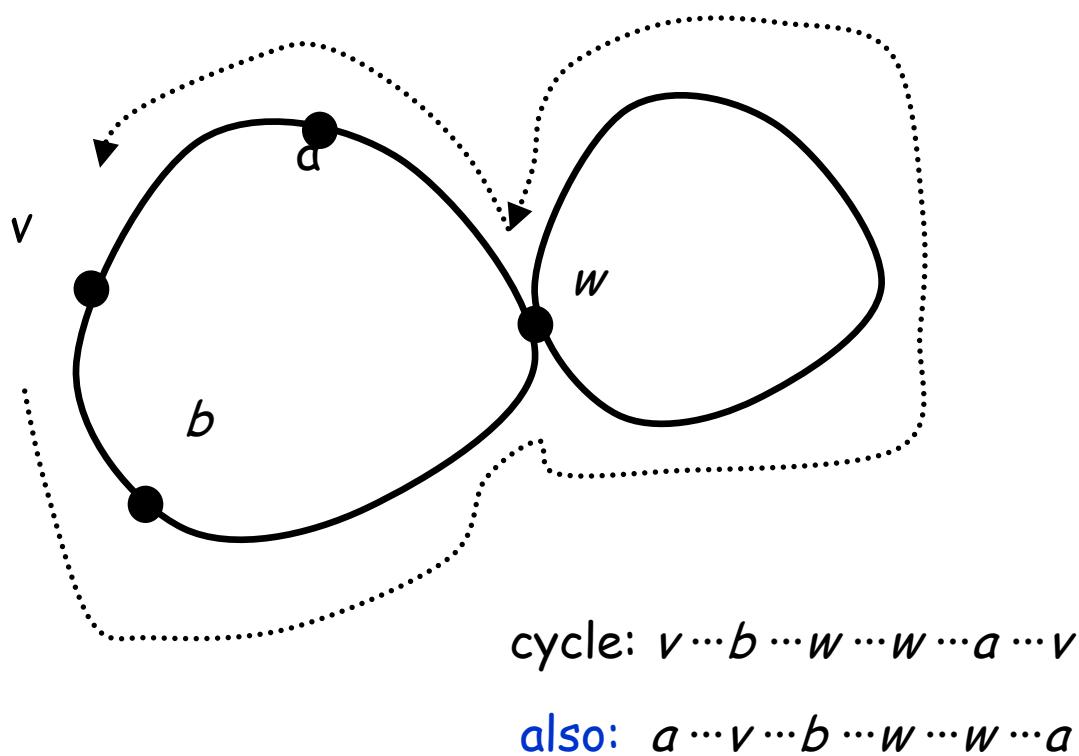
Every graph consists of separate connected pieces called *connected components*



So a graph is *connected* if and only if it has only **1** *connected component*.

Cycles

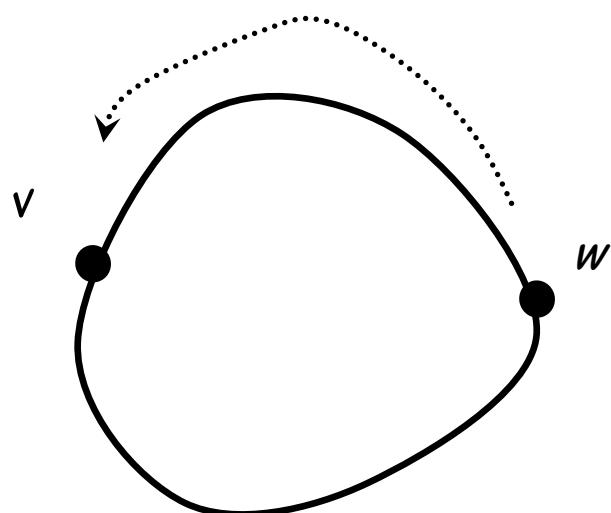
A *cycle* is a path that begins and ends with same vertex.



Simple Cycles

A simple *cycle* is a cycle that doesn't cross itself

In a simple cycle, every vertex is of degree exactly 2.



cycle: $v \dots w \dots v$

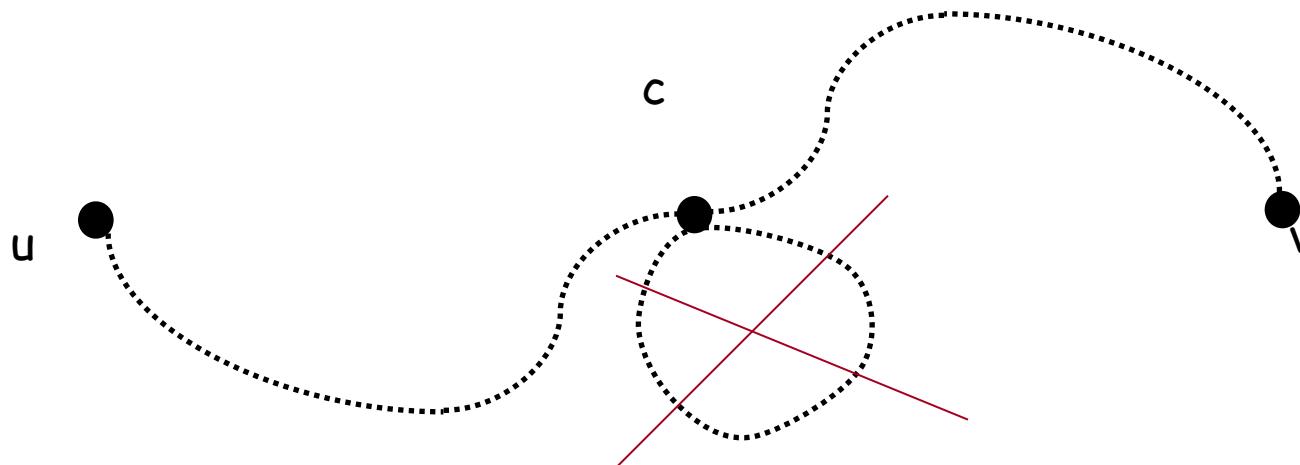
also: $w \dots v \dots w$

Shortest Paths

A path between u and v is a *shortest path* if among all u - v paths it uses the minimum number of edges.

Is a shortest path between two vertices always simple?

Idea: remove the cycle will make the path shorter.



1.6 Connected graphs

Definition.

A **walk** (path) in a graph G is an alternating sequence

$W: v_0, e_1, v_1, e_2, v_2, \dots, v_{n-1}, e_n, v_n$ ($n \geq 0$)

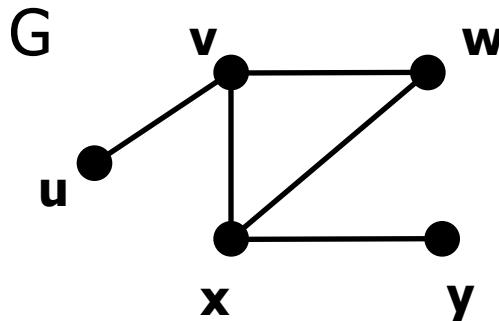
of vertices and edges, where $e_i = v_{i-1}v_i$, $\forall i$.

(W is also called a v_0 - v_n walk)

W is said to have **length n** .

A **trail** is a walk without repeated edges.

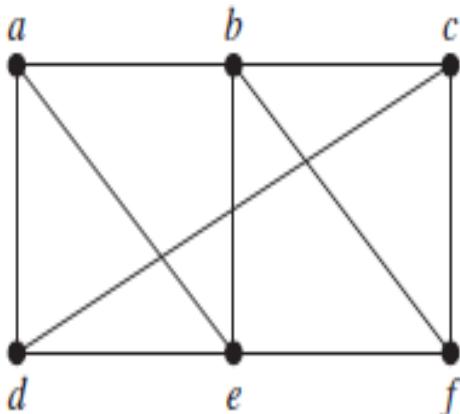
A **simple path** is a walk without repeated vertices.



walk: x, w, v, x, w

trail: x, w, v, x, y

Simple path: x, w, v



EXAMPLE

In the simple graph shown in Figure , a, d, c, f, e is a simple path of length 4, because $\{a, d\}$, $\{d, c\}$, $\{c, f\}$, and $\{f, e\}$ are all edges. However, d, e, c, a is not a path, because $\{e, c\}$ is not an edge. Note that b, c, f, e, b is a circuit of length 4 because $\{b, c\}$, $\{c, f\}$, $\{f, e\}$, and $\{e, b\}$ are edges, and this path begins and ends at b . The path a, b, e, d, a, b , which is of length 5, is not simple because it contains the edge $\{a, b\}$ twice. ◀

Theorem 1.3

Every $u-v$ walk in a graph contains a $u-v$ simple path.

Definition

- (1) A **cycle** is a walk $v_0, v_1, v_2, \dots, v_{n-1}, v_n$ in which $n \geq 3$, $v_0 = v_n$, and $v_1, v_2, \dots, v_{n-1}, v_n$ are distinct. (**n -cycle**)
- (2) A $u-v$ walk is **closed** if $u=v$. (**closed walk**)
- (3) A nontrivial closed trail is called a **circuit**.

Definition

- (1) Let $u, v \in V(G)$, u is connected to v if \exists u - v path.
- (2) G is connected if u is connected to v $\forall u, v \in V(G)$, otherwise, G is called disconnected.
- (3) A subgraph H of G is a component of G if H is a maximal connected subgraph of G .
- (4) The number of components of G is denoted by $k(G)$.

Note. “is connected to” is an equivalence relation

Counting Paths Between Vertices

The number of paths between two vertices in a graph can be determined using its adjacency matrix.

Let G be a graph with adjacency matrix \mathbf{A} with respect to the ordering v_1, v_2, \dots, v_n of vertices of the graph (with directed or undirected edges, with multiple edges and loops allowed). The number of different paths of length r from v_i to v_j , where r is a positive integer, equals the (i, j) th entry of \mathbf{A}^r .

Proof: The theorem will be proved using mathematical induction. Let G be a graph with adjacency matrix \mathbf{A} (assuming an ordering v_1, v_2, \dots, v_n of the vertices of G). The number of paths from v_i to v_j of length 1 is the (i, j) th entry of \mathbf{A} , because this entry is the number of edges from v_i to v_j .

Assume that the (i, j) th entry of \mathbf{A}^r is the number of different paths of length r from v_i to v_j . This is the inductive hypothesis. Because $\mathbf{A}^{r+1} = \mathbf{A}^r \mathbf{A}$, the (i, j) th entry of \mathbf{A}^{r+1} equals

$$b_{i1}a_{1j} + b_{i2}a_{2j} + \cdots + b_{in}a_{nj},$$

where b_{ik} is the (i, k) th entry of \mathbf{A}^r . By the inductive hypothesis, b_{ik} is the number of paths of length r from v_i to v_k .

A path of length $r + 1$ from v_i to v_j is made up of a path of length r from v_i to some intermediate vertex v_k , and an edge from v_k to v_j . By the product rule for counting, the number of such paths is the product of the number of paths of length r from v_i to v_k , namely, b_{ik} , and the number of edges from v_k to v_j , namely, a_{kj} . When these products are added for all possible intermediate vertices v_k , the desired result follows by the sum rule for counting. 

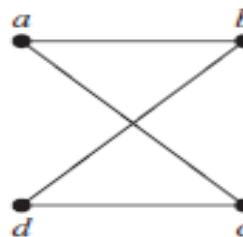


FIGURE 8
Graph G .

EXAMPLE 15 How many paths of length four are there from a to d in the simple graph G in Figure 8?

Solution: The adjacency matrix of G (ordering the vertices as a, b, c, d) is

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

Hence, the number of paths of length four from a to d is the $(1, 4)$ th entry of \mathbf{A}^4 .

$$\mathbf{A}^4 = \begin{bmatrix} 8 & 0 & 0 & 8 \\ 0 & 8 & 8 & 0 \\ 0 & 8 & 8 & 0 \\ 8 & 0 & 0 & 8 \end{bmatrix},$$

there are exactly eight paths of length four from a to d . By inspection of the graph, we see that $a, b, a, b, d; a, b, a, c, d; a, b, d, b, d; a, b, d, c, d; a, c, a, b, d; a, c, a, c, d; a, c, d, b, d;$ and a, c, d, c, d are the eight paths of length four from a to d . ◀