4 CHAPTER Number Theory and Cryptography

4.1.2 Division

- When one integer is divided by a second nonzero integer, the quotient mayor may not be an integer.
- For example, 12⁄3 = 4 is an integer, whereas 11⁄4 = 2.75 is not.

Definition:

If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$ (or equivalently, if $\frac{b}{a}$ is an integer). When a divides b we say that a is a factor or divisor of b, and that b is a multiple of a. The notation $a \mid b$ denotes that a divides b. We write $a \nmid b$ when a does not divide b.

- Remark: We can express $a \mid b$ using quantifiers as $\exists c(ac = b)$, where the universe of discourse is the set of integers.

Example: Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Solution:

- $3 \nmid 7$, because 7⁄3 is not an integer.
- On the other hand, $3 \mid 12$ because 12⁄3 = 4

Properties of Divisibility

Theorem 1: Let a, b, and c be integers, where $a \neq 0$. Then

(i) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

(ii) if $a \mid b$, then $a \mid bc$ for all integers c;

(iii) if $a \mid b$ and $b \mid c$, then $a \mid c$

Proof

i. **:** if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$

- from the definition of divisibility we get:
- $b=au$ and $c=av$ where u,v are two integers. Then$(b+c) = au + av = a(u+v)$

- **Thus a divides b+c.**

ii. : if a | b then a | bc for all integers c

- If a | b, then there is some integer u such that b = au.
- Multiplying both sides by c gives us bc = auc, so by definition, a | bc.

- **Thus a divides bc.**

Corollary 1: If a, b, and c are integers, where a ≠ 0, such that a | b and a | c, then

a| mb + nc whenever m and n are integers.

Proof:

We will give a direct proof. By part (ii) of Theorem 1 we see that a | mb and a | nc whenever m and n are integers. By part (i) of Theorem 1 it follows that a | mb + nc

Primes

Definition:

A positive integer p that is greater than 1 and that is divisible only by 1 and byitself (p) is called **a prime**.

Examples: 2, 3, 5, 7, …

1 | 2 and 2 | 2, 1 |3 and 3 | 3, etc

Definition:

A positive integer that is greater than 1 and is not a prime is called **a composite**

Examples : 4, 6, 8, 9, …Why?

2 | 4

3 | 6 or 2 | 6

2 | 8 or 4 | 8

3 | 9

Fundamental theorem of Arithmetic:

Any positive integer greater than 1 can be expressed as a product of prime numbers.

Examples:

- 12 = 2*2*3
- 21 = 3*7

- Process of finding out factors of the product:

factorization.Factorization of composites to primes:

- 100 = 2*2*5*5 = 2^2*5^2
- 99 = 3*3*11 = 3^2 *11

- **How to determine whether the number is a prime or a composite?**

- **Simple approach (1):**

- Let *n* be a number. To determine whether it is a prime we can test if any number $x < n$ divides it. If yes it is a composite. If we test all numbers $x < n$ and do not find the proper divisor then *n* is a prime.

Example 1:

- Assume we want to check if 17 is a prime?
- The approach would require us to check:
- 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16

- **Is this the best we can do?**
- **No.** The problem here is that we try to test all the numbers. But this is not necessary.
- **Idea:** Every composite factorizes to a product of primes. So it is sufficient to test only the primes $x < n$ to determine the primality of *n*.

Approach 2:

- Let *n* be a number. To determine whether it is a prime we can test if

any prime number x < n divides it. If yes it is a composite.
If we test all primes $x < n$ and do not find a proper divisor then n is a prime.

Example 2: Is 31 a prime?

- Check if 2,3,5,7,11,13,17,23,29 divide it
- It is a prime !!

Example 3: Check if Is 91 a prime number?

- Easy primes 2,3,5,7,11,13,17,19 …
- But how many primes are there that are smaller than 91?

Caveat:

- If n is relatively small the test is good because we can enumerate(memorize) all small primes
  But if n is large there can be larger not obvious primes

Theorem 2: If n is a composite then n has a prime divisor less than or equal to $\sqrt{n}$

Approach 3:

- Let n be a number. To determine whether it is a prime we can test if any prime number $x \leq \sqrt{n}$ divides it.

Example 4: **Is 101 a prime?**

Primes smaller than or equal to $\sqrt{101} \approx 10.04987$ are: 2,3,5,7

- 101 is not divisible by any of them
- **Thus 101 is a prime**

- **Question:** How many primes are there?

Theorem 3: There are infinitely many primes.

The Division Algorithm

Theorem 4: **[The Division Algorithm]** Let a be an integer and d a positive integer. Then there are unique integers, q and r, with $0 \leq r < d$, such that

$$\mathbf{a = dq + r}.$$

Definition:

In the equality given in the division algorithm, **d** is called the **divisor**, **a** is called the **dividend**, **q** is called the **quotient**, and r is called the remainder. This notation is used to express the quotient and remainder: **q = a div d**, **r = a mod d.**

Example 5:

a= 14, d = 3

14 = 3*4 + 2

14/3=3.666

14 div 3 = 4

14 mod 3 = 2

Greatest common divisor

Definition:

Let a and b are integers, not both 0. Then the largest integer d such that d | a and d | b is called **the greatest common divisor** of a and b. The greatest common divisor is denoted as gcd(a,b).

Examples:

- gcd(24,36) = ?
- Check 2,3,4,6,12 gcd(24,36) = 12
- gcd(11,23) = ?

A systematic way to find the gcd using factorization:

- Let **a**=$p_1^{a_1}$ $p2^{a_2}$ $p_3^{a_3}$ $\ldots_k^{a_k}$ and **b**= $p_1^{b_1}$ $p_2^{b_2}$ $p_2^{b_3}$ … $p_k^{b_k}$
- gcd(a,b)= $p_1^{\min(a1,b1)}$ $p_2^{\min(a2,b2)}$ $p_3^{\min(a3,b3)}$ … $p_k^{\min(ak,bk)}$

Example 6 :

- gcd(24,36) = ?
- 24 = 2*2*2*3=$2^{3*}3$

- 36= $2*2*3*3=2^2 * 3^2$
- gcd(24,36) $=2^2 * 3 =$ **12**

Least common multiple

Definition:

Let a and b are two positive integers. The least common multiple of a and b is the smallest positive integer thatis divisible by both a and b. The **least common multiple** is denoted as **lcm(a,b).**

Example 7:

- **What is lcm(12,9) =?**
- Give me a common multiple: … 12*9= 108
- **Can we find a smaller number?**
- **Yes.** Try 36. Both 12 and 9 cleanly divide 36

A systematic way to find the lcm using factorization:

- Let **a**$=p_1{}^{a_1}\ p2^{a_2}\ p_3{}^{a_3}\ \ldots_k{}^{a_k}$ and **b**$=p_1{}^{b_1}\ p_2{}^{b_2}\ p_2{}^{b_3}\ \ldots\ p_k{}^{b_k}$
- lcm(a,b)$=p_1{}^{\max(a1,b1)}\ p_2{}^{\max(a2,b2)}\ p_3{}^{\max(a3,b3)}\ \ldots\ p_k{}^{\max(ak,bk)}$

Example 8:

- **What is lcm(12,9) =?**
- $12 = 2*2*3=2^2*3$
- $9=3*3 =3^2$
- **lcm(12,9)** $= 2^2 * 3^2 = 4 * 9 =$ **36**

Euclid algorithm

Finding the greatest common divisor requires factorization

Factorization can be cumbersome and time consuming since we need to find all factors the two integers that can be very large.

- Luckily a more efficient method for computing the gcd is the **Euclid's algorithm.**

Example 9:

- Find the greatest common divisor of 666 and 558

Solution

gcd(666,558)	666=1*558 + 108
= gcd(558,108)	558=5*108 + 18
= gcd(108,18)	108=6*18 + 0
= **18**	

Example 10:

- Find the greatest common divisor of 286 and 503:

Solution

• gcd(503,286)	503=1*286 + 217
=gcd(286, 217)	286=1*217 + 69
=gcd(217, 69)	217 = 3*69 + 10
= gcd(69,10)	69 = 6*10 + 9
=gcd(10,9)	10=1*9 + 1
= gcd(9,1) =**1**	

Modular arithmetic

In computer science we often care about the remainder of an integer when it is divided by some positive integer.

Problem: Assume that it is a midnight. What is the time on the 24hour clock after 50 hours?

Answer: the result is 2 am

How did we arrive to the result:

- Divide 50 with 24. The reminder is the time on the 24 hour clock.50= 2*24 + 2

  so the result is 2 am.

Congruency

Definition:

If a and b are integers and m is a positive integer, then **a is congruent to b modulo n** if m divides a-b. We use the notation **a = b (mod m)** to denote the congruency. If a and b are not congruent we write a ≠ b (mod m).

Theorem 5. If a and b are integers and m a positive integer. Then a=b (**mod** m) if and only if **a** mod **m** = **b** mod **m**.

Example 11: Determine if 17 is congruent to 5 modulo 6?

Solution:

17 mod 6 = **5**
5 mod 6 = **5**

Thus 17 is congruent to 5 modulo 6.

Theorem 6. Let **m** be a positive integer. The integers **a** and **b** are congruent modulo m if and only if there exists an integer k such that **a**=b+**mk**.

Theorem 7. Let **m** be a positive integer. If **a**=b (mod **m**) and **c**=**d**(mod **m**) then:

a+c = **b+d** (mod **m**) and **ac**=**bd** (mod **m**).

Modular arithmetic in Computer Science

Modular arithmetic and congruencies are used in Science:

- **Pseudorandom number generators**
- **Hash functions**
- **Cryptology**

Pseudorandom number generators

- **Some problems we want to program need to simulate a random choice.**
- **Examples: flip of a coin, roll of a dice**
- **We need a way to generate random Outcomes**
- **Basic problem:**
  - assume outcomes: 0, 1, .. N
  - generate the random sequences of outcomes
  - Pseudorandom number generators let us generate sequences that look random
  - **Next:** linear congruential method

Linear congruential method

- We choose 4 numbers:
- the modulus m,
- multiplier a,
- increment c, and
- seed x_0,

such that $2 \leq a < m$, $0 \leq c < m$, $0 \leq x_0 < m$.

- We generate a sequence of numbers x_1, x_2 x_3 ... x_n ... such that $0 \leq x_n < m$ for all n by successively using the congruence:
  - $x_{n+1} = (a.x_n + c) \bmod m$

Example 12:

- Assume : $m=9, a=7, c=4, x_0 = 3$

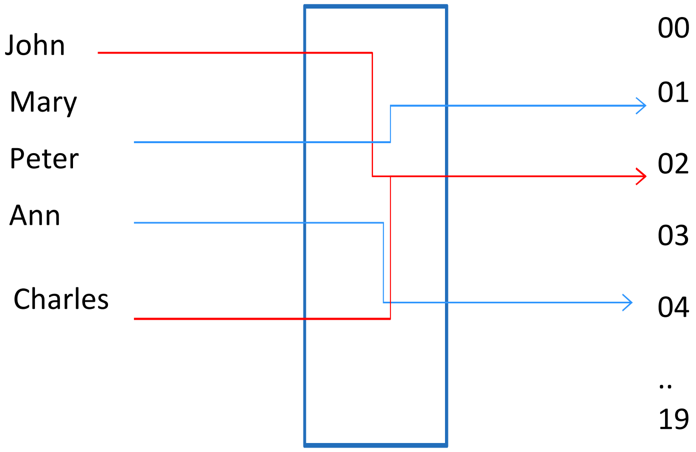
- $x_1 = 7*3+4 \bmod 9 = 25 \bmod 9 = 7$
- $x_2 = 53 \bmod 9 = 8$
- $x_3 = 60 \bmod 9 = 6$
- $x_4 = 46 \bmod 9 = 1$
- $x_5 = 11 \bmod 9 = 2$
- $x_6 = 18 \bmod 9 = 0$
- ....

Hash functions

- A ***hash function*** is an algorithm that maps data of arbitrary length to data of afixed length.
- The values returned by a hash function are called **hash values** or **hash codes.**

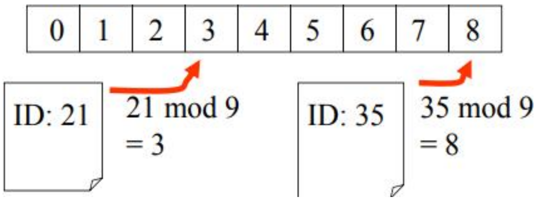
For Example :

Hash function



- **Problem:** Given a large collection of records, how can we store and find a recordquickly?
- **Solution:** Use a hash function calculate the location of the record based on therecord's ID.
- **Example 1:** A common hash function is
  - $h(k) = k$ **mod** m,

where m is the number of available storage locations.



An example of a hash function that maps integers (including verylarge ones) to a subset of integers 0, 1, .. m-1 is:

- **h(k) = k mod m**

Example 2: Assume we have a database of employees, each with a unique ID – a social security number that consists of 8 digits. We want to store the records in a smaller table with m entries. Using h(k) function we can map a social security number in the database of employees to indexes in the table.

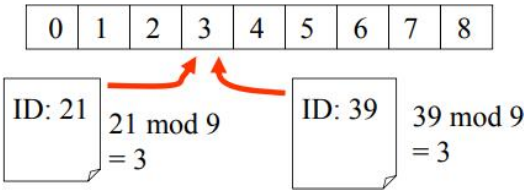
Assume: h(k) = k mod 111

Then:

h(064212848) = 064212848 mod 111 = 14

h(037149212) = 037149212 mod 111 = 65

- **Problem:** two documents mapped to the same location



- **Solution :** move the next available location

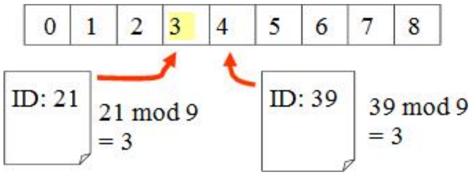
– Method is represented by a sequence of hash functions to

Try

$h_0(k) = k \textbf{ mod } m\ h_1(k) = (k+1) \textbf{ mod } m$

…

$h_m(k) = (k+m) \textbf{ mod } m$



There are many other ways to resolve collisions that are discussed in the references on hashing functions given at the end of the book.

Cryptology

Encryption of messages.

- **Caesar cipher:**
- Shift letters in the message by 3, last three letters mapped to the first 3 letters, e.g. A is shifted to D, X is shifted to A

How to represent the idea of a shift by 3?

- There are 26 letters in the alphabet. Assign each of them a number from 0,1, 2, 3, .. 25 according to the alphabetical order.
- **Coding of letters:**

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:
  - $f(p) = (p + 3) \bmod 26$
- **Encrypt message:**

– **I LIKE DISCRETE MATH**

– **L 0LNH GLYFUHVH PDVK.**

How to decode the message ?

  - $\mathbf{f^{-1}(p) = (p-3) \bmod 26}$

4.2 Integer Representations and Algorithms

Representations of Integers

- In the modern world, we use *decimal,* or *base* 10, *notation* to represent integers. For example when we write 965, we mean

  $965= 9\cdot10^2 + 6\cdot10^1 + 5\cdot10^0$.
- We can represent numbers using any base b, where b is a positive integer greater than 1.
- The bases $b = 2$ (*binary*), $b = 8$ (*octal*), and $b= 16$ (*hexadecimal*) are important for computing and communications
- The ancient Mayans used base 20 and the ancient Babylonians used base 60.

Base *b* Representations

- We can use positive integer b greater than 1 as a base

Theorem 1: Let b be a positive integer greater than 1. Then if n isa positive integer, it can be expressed uniquely in the form:

$$n = a_k b^k + a_{k-1} b^{k-1} + \dots. + a_1 b + a_0$$

where k is a nonnegative integer, $a_0, a_1, \dots.\ a_k$ are nonnegative integers less than b, and $a_k \neq 0$. The a_j, $j = 0,\dots,k$ are called the base-b digits of therepresentation.

- The representation of n given in **Theorem 1** is called the ***base b expansionof n*** and is denoted by $\boldsymbol{(a_k a_{k-1} \dots. a_1 a_0)_b}$.

We usually omit the subscript 10 for base 10 expansions.

Binary Expansions

- Most computers represent integers and do arithmetic with binary (base 2) expansions of integers.
- In these expansions,the only digits used are 0 and 1.

Example 1:

What is the decimal expansion of the integer that has$(1\ 01011111)_2$ as its binary expansion?

Solution:

$(1\ 0101\ 1111)_2 = 1\cdot2^8 + 0\cdot2^7 + 1\cdot2^6 + 0\cdot2^5 + 1\cdot2^4 + 1\cdot2^3$

$+ 1\cdot2^2 + 1\cdot2^1 + 1\cdot2^0 = 351.$

Example 2: What is the decimal expansion of the integer that has $(11011)_2$ as its binary expansion?

Solution: $(11011)_2 = 1\cdot2^4 + 1\cdot2^3 + 0\cdot2^2 + 1\cdot2^1 + 1\cdot2^0 = 27$

Octal Expansions

- The octal expansion (base 8) uses the digits {0,1,2,3,4,5,6,7}.

Example 3: What is the decimal expansion of the number with octalexpansion $(7016)_8$?

Solution: $7\cdot8^3 + 0\cdot8^2 + 1\cdot8^1 + 6\cdot8^0 = 3598$

Example 4: What is the decimal expansion of the number with octal expansion $(111)_8$?

Solution: $1\cdot8^2 + 1\cdot8^1 + 1\cdot8^0 = 64 + 8 + 1 = 73$

Hexadecimal Expansions

- The hexadecimal expansion uses 16 digits: {0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F}.
  - The letters A through F represent the decimal numbers 10 through 15.

Example 5: What is the decimal expansion of the number with hexadecimal expansion $(2AE0B)_{16}$?

Solution:

$2\cdot16^4 + 10\cdot16^3 + 14\cdot16^2 + 0\cdot16^1 + 11\cdot16^0 = 175627$

Example 6: What is the decimal expansion of the number with hexadecimal expansion $(E5)_{16}$?

Solution: $14\cdot16^1 + 5\cdot16^0 = 224 + 5 = 229$

Base Conversion

- To construct the base *b* expansion of an integer *n*:
  - Divide *n* by *b* to obtain a quotient and remainder.

    $$n = bq_0 + a_0 \qquad 0 \le a_0 \le b$$

  - The remainder, a_0 , is the rightmost digit in the base *b* expansion of *n*. Next, divide q_0 by $b.q_0$

    $$b.q_0 = bq_1 + a_1 \qquad 0 \le a_1 \le b$$

  - The remainder, a_1, is the second digit from the right in the base *b* expansion of *n*.
  - Continue by successively dividing the quotients by *b*, obtaining the additional base *b* digits as the remainder.
  - The process terminates when the quotient is 0.

Example 7: Find the octal expansion of $(12345)_{10}$

Solution: Successively dividing by 8 gives:

$$12345 = 8 \cdot 1543 + 1$$
$$1543 = 8 \cdot 192 + 7$$
$$192 = 8 \cdot 24 + 0$$
$$24 = 8 \cdot 3 + 0$$
$$3 = 8 \cdot 0 + 3$$

- The remainders are the digits from right to left yielding$(30071)_8$.

Chapter 9 Relations

9.1 Relations and Their Properties

Definition: Binary relation

Let A and B be two sets. A **binary relation from A toB** is a subset of a Cartesian product A x B.

- Let R $\subseteq$ A x B means R is a set of ordered pairs of the form (a,b)where a $\in$ A and b $\in$ B.
- We use the notation **a R b to denote (a,b)** $\in$ **R** and **a R b todenote (a,b)** $\notin$ **R**. If **a R b**, we say a is related to b by R

Example 1: Let A={a,b,c} and B={1,2,3}.

- Is R={(a,1),(b,2),(c,2)} a relation from A to B? **Yes.**
- Is Q={(1,a),(2,b)} a relation from A to B? **No.**
- Is P={(a,a),(b,c),(b,a)} a relation from A to A? **Yes**

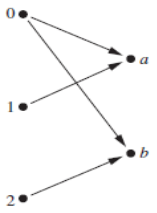
Representing binary relations

- We can graphically represent a binary relation R as follows:
  - if **a R b** then draw an arrow from a to b.

$$\mathbf{a} \rightarrow \mathbf{b}$$

Example 2:

- Let A = {0, 1, 2}, B = {a,b}
  and R = { (0,a), (0,b), (1,a), (2,b) } is a relation from *A* to *B*.
- **Graph:**



- We can represent a binary relation R by a **table** showing(marking) the ordered pairs of R.

Example 3:

- Let A = {0, 1, 2}, B = {u,v} and R = { (0,u), (0,v), (1,v), (2,u) }
- **Table:**

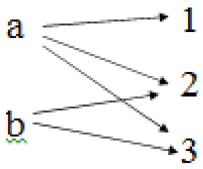
R	u	v
0	x	x
1		x
2	x	

or

R	u	v
0	1	1
1	0	1
2	1	0

Functions as Relations

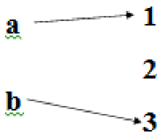
- Relations represent **one to many relationships** betweenelements in A and B.
- **For example:**



- What is the difference between a **relation and a function from A to B**?
- A function defined on sets A, B

A → B assigns to each element in the domain set A exactly one element from B.

- So it is **a special relation.**



Relation on the set

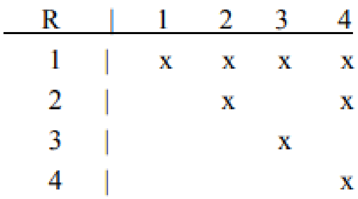
Definition:

A relation on the set A is a relation from A to itself.

Example 4:

- Let A = {1,2,3,4} and R_{div} = {(a,b)| a divides b}
- What does R_{div} consist of?

R_{div} = {(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)}

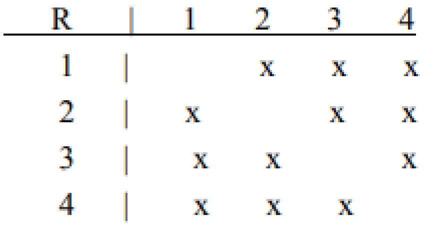


R	1	2	3	4
1	x	x	x	x
2		x		x
3			x	
4				x

Example 5:

- Let A = {1,2,3,4}.
- Define a $R_{\neq}$ b if and only if a ≠ b.

$R_{\neq}$ ={(1,2),(1,3),(1,4),(2,1),(2,3),(2,4),(3,1),(3,2),(3,4),(4,1),(4,2),(4,3)}



R	1	2	3	4
1		x	x	x
2	x		x	x
3	x	x		x
4	x	x	x	

Theorem: The number of binary relations on a set A, where | A | = n is : 2^{n^2}

Proof

If | A | = n then the cardinality of the Cartesian product

| A x A | = n^2.

- R is a binary relation on A if R ⊆ A x A (that is, R is a subsetof A x A).
- The number of subsets of a set with k elements : 2^k
- The number of subsets of A x A is : $2^{|AxA|} = 2^{n^2}$

Example 6: Let A = {1,2}

- What is A x A ?

A x A = **{(1,1),(1,2),(2,1),(2,2)}**

- **List of possible relations (subsets of A x A):**
  - ∅
  - {(1,1)} {(1,2)} {(2,1)} {(2,2)}
  - {(1,1), (1,2)} {(1,1),(2,1)}
    {(1,1),(2,2)} {(1,2),(2,1)}
    {(1,2),(2,2)} {(2,1),(2,2)}
  - {(1,1),(1,2),(2,1)}
    {(1,1),(1,2),(2,2)}
    {(1,1),(2,1),(2,2)}
    {(1,2),(2,1),(2,2)}
  - {(1,1),(1,2),(2,1),(2,2)}

  - Use formula: **2^4 = 16**

Properties of relations

Definition:(reflexive relation) :

A relation R on a set A is called **reflexive** if (a,a) ∈ R for every element a ∈ A.

Example 7:

- Assume relation R_{div} ={(a b), if a |b} on A = {1,2,3,4}
- **Is R_{div} reflexive?**
- R_{div} = {(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)}
- **Answer: Yes.** (1,1), (2,2), (3,3), and (4,4) ∈ R_{div} .

1 1 1 1

$$MR_{div} = \begin{matrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}$$

- **A relation R is reflexive** if and only if MR has 1 in everyposition on its main diagonal.

Example 8:

- Relation R_{fun} on A = {1,2,3,4} defined as:
  - R_{fun} = {(1,2),(2,2),(3,3)}.
- **Is R_{fun} reflexive?**

  No. It is not reflexive since $(1,1) \notin R_{fun}$.

Definition:(irreflexive relation) :

A relation R on a set A is called **irreflexive** if **$(a,a) \notin$ R for every $a \in$ A.**

Example 9:

- Assume relation $R_{\neq}$ on A={1,2,3,4}, such that **a $R_{\neq}$ b** if and onlyif $a \neq b$.
- **Is $R_{\neq}$ irreflexive?**
- **$R_{\neq}$={(1,2),(1,3),(1,4),(2,1),(2,3),(2,4),(3,1),(3,2),(3,4),(4,1),(4,2),(4,3)}**
- **Answer:** Yes. Because (1,1),(2,2),(3,3) and $(4,4) \notin R_{\neq}$
- **A relation R is irreflexive** if and only if MR has 0 in everyposition on its main diagonal.

$$MR = \begin{matrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{matrix}$$

Example 10:

- R_{fun} on A = {1,2,3,4} defined as:
    - R_{fun} = {(1,2),(2,2),(3,3)}.
- **Is Rfun irreflexive?**
- **Answer: No**. Because (2,2) and (3,3) ∈ R_{fun}

Definition:(symmetric relation):

A relation R on a set A is called **symmetric** if ∀ a, b ∈ A (a,b)∈ R → (b,a) ∈ R.

Example 11:

- R_{div} ={(a b), if a |b} on A = {1,2,3,4}
- **Is R_{div} symmetric?**
- Rdiv = {(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)}
- **Answer: No.** It is not symmetric since (1,2) ∈ R_{div} but (2,1) ∉ R_{div}.

Example 12:

- R≠ on A={1,2,3,4}, such that **a R≠ b** if and only if a ≠ b.
- **Is R≠ symmetric ?**
- **R≠={(1,2),(1,3),(1,4),(2,1),(2,3),(2,4),(3,1),(3,2),(3,4),(4,1),(4,2),(4,3)}**
- **Answer: Yes. If** (a,b) ∈ R≠ → (b,a) ∈ R≠

- **A relation R is symmetric** if and only if $m_{ij} = m_{ji}$ for all i,j.

$$MR = \begin{matrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{matrix}$$

Example 13:

- Relation R_{fun} on A = {1,2,3,4} defined as:
    - R_{fun} = {(1,2),(2,2),(3,3)}.

- **Is R_{fun} symmetric?**

  Answer: No. For $(1,2) \in R_{fun}$ there is no $(2,1) \notin R_{fun}$

Definition:(anti-symmetric relation):

A relation on a set A iscalled **anti-symmetric** if

- $[(a,b) \in R \text{ and } (b,a) \in R] \rightarrow a = b$ where $a, b \in A$.

- **Example 14:**
- Relation R_{fun} on $A = \{1,2,3,4\}$ defined as:
  - $R_{fun} = \{(1,2),(2,2),(3,3)\}$.
- **Is R_{fun} anti-symmetric?**
- **Answer: Yes.** It is anti-symmetric

$$MR_{fun} = \begin{matrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{matrix}$$

- A relation is **antisymmetric** if and only if $m_{ij} = 1 \rightarrow m_{ji} = 0$ for $i \neq j$.

Definition:(transitive relation):

A relation R on a set A is called **transitive** if

- $[(a,b) \in R \text{ and } (b,c) \in R] \rightarrow (a,c) \in R$ for all $a, b, c \in A$.

Example 15:

- $R_{div} = \{(a\ b), \text{ if } a\ |b\}$ on $A = \{1,2,3,4\}$
- $R_{div} = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)\}$
- **Is R_{div} transitive?**
- **Answer: Yes**

Example 16:

- $R_{\neq}$ on A={1,2,3,4}, such that **a $R_{\neq}$ b** if and only if a ≠ b.
- **$R_{\neq}$={(1,2),(1,3),(1,4),(2,1),(2,3),(2,4),(3,1),(3,2),(3,4),(4,1),(4,2),(4,3)}**
- **Is $R_{\neq}$ transitive?**
- **Answer: No.** It is not transitive since (1,2) ∈ R and (2,1) ∈ R but (1,1) is not an element of R.

- ## Example 17:

- Relation R_{fun} on A = {1,2,3,4} defined as:
  - R_{fun} = {(1,2),(2,2),(3,3)}.
- **Is R_{fun} transitive?**
- **Answer: Yes.** It is transitive.

Properties of relations on A:

- Reflexive
- Irreflexive
- Symmetric
- **Anti-symmetric**
- **Transitive**

Combining relations

Definition: Let A and B be sets. A **binary relation from A to B** isa subset of a Cartesian product A x B.

- Let R $\subseteq$ A x B means R is a set of ordered pairs of the form (a,b)where a $\in$ A and b $\in$ B.

Combining Relations

- **Relations are sets → combinations via set operations**
- Set operations of: **union, intersection, difference and symmetric difference.**

Example:

- Let A = {1,2,3} and B = {u,v} and
- R1 = {(1,u), (2,u), (2,v), (3,u)}
- R2 = {(1,v),(3,u),(3,v)}

What is:

- R1 $\cup$ R2 = {(1,u),(1,v),(2,u),(2,v),(3,u),(3,v)}
- R1 $\cap$ R2 = {(3,u)}
- R1 - R2 = {(1,u),(2,u),(2,v)}
- R2 - R1 = {(1,v),(3,v)}

9. 3 Representing Relations using matrices

- **Question:** Can the relation be formed by taking the union or intersection or composition of two relations R_1 and R_2 be represented in terms of matrix operations?
- **Answer: Yes**

Example 1: Suppose that A = {1, 2, 3} and B = {1, 2}. Let R be the relation from A to B containing (a, b) if a ∈ A, b ∈ B, and a > b. What is the matrix representing R if $a_1 = 1$, $a_2 = 2$, and $a_3 = 3$, and $b_1 = 1$ and $b_2 = 2$?

Solution: Because R = {(2, 1), (3, 1), (3, 2)}, the matrix for R is

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

Definition:

The **join,** denoted by ∨, of two m-by-n matrices $(a_{ij})$and (b_{ij}) of 0s and 1s is an m-by-n matrix (m_{ij}) where

- $m_{ij} = a_{ij} \vee b_{ij}$ for all i,j

= pairwise or (disjunction)

Example 2

Let A = {1,2,3} and B = {u,v}

R_1 = {(1,u), (2,u), (2,v), (3,u)}

R_2 = {(1,v),(3,u),(3,v)}

- $$\mathbf{MR_1} = \begin{matrix} \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{matrix} \qquad \mathbf{MR_2} = \begin{matrix} \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} \end{matrix} \qquad \mathbf{M(R_1 \vee R_2)} = \begin{matrix} \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} \end{matrix}$$

Definition:

The **meet,** denoted by ∧ , of two m-by-n matrices $(a_{ij})$and (b_{ij}) of 0s and 1s is an m-by-n matrix (m_{ij}) where

- $m_{ij} = a_{ij} \wedge b_{ij}$ for all i,j

= **pairwise and (conjunction)**

Example 3:

- Let A = {1,2,3} and B = {u,v}

  R_1 = {(1,u), (2,u), (2,v), (3,u)}
- R_2 = {(1,v),(3,u),(3,v)}

- $\mathbf{MR_1 = \begin{matrix} 1 & 0 \\ 1 & 1 \\ 1 & 0 \end{matrix}}$ $\quad$ $\mathbf{MR_2 = \begin{matrix} 0 & 1 \\ 0 & 0 \\ 1 & 1 \end{matrix}}$ $\quad$ $\mathbf{MR_1 \wedge MR_2 = \begin{matrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{matrix}}$

Definition: Composite of relations

Let R be a relation from a set A to a set B and S a relation from B to a set C. The **composite of R and S** is the relation consisting of the ordered pairs (a,c) where a ∈ A and c ∈ C, and for which there is a b ∈ B such that (a,b) ∈ R and (b,c) ∈ S. We denote the composite of R and S by S o R.

Example 4:

- Let A = {1,2,3}, B = {0,1,2} and C = {a,b}.
- R = {(1,0), (1,2), (3,1),(3,2)}
- S = {(0,b),(1,a),(2,b)}
- S o R = {(1,b),(3,a),(3,b)}

Implementation of composite

Definition:

The **Boolean product, denoted by ⊙,** of an m-by-n matrix (a_{ij}) and n-by-p matrix (b_{jk}) of 0s and 1s is an m-by-p matrix (m_{ik}) where

$$m_{ik} = \begin{cases} 1, \text{ if } a_{ij} = 1 \text{ and } b_{jk} = 1 \text{ for some } k=1,2,\ldots,n \\ 0, \text{ otherwise} \end{cases}$$

Example 5:

- Let A = {1,2}, B= {1,2,3} C = {a,b}
- R = {(1,2),(1,3),(2,1)} is a relation from A to B
- S = {(1,a),(3,b),(3,a)} is a relation from B to C.
- S o R = {(1,b),(1,a),(2,a)}

$$M_R = \begin{matrix} 0 & 1 & 1 \\ 1 & 0 & 0 \end{matrix} \qquad M_S = \begin{matrix} 1 & 0 \\ 0 & 0 \\ 1 & 1 \end{matrix}$$

$$M_R \odot M_S = \begin{matrix} 1 & 1 \\ 1 & 0 \end{matrix}$$

$$M_{S \circ R} = \begin{matrix} 1 & 1 \\ 1 & 0 \end{matrix}$$

Definition:

Let R be a relation on a set A. The **powers R^n**, n =1,2,3,... is defined inductively by

- **$R^1 = R$** and **$R^{n+1} = R^n \circ R$**.

Example 6:

- R = {(1,2),(2,3),(2,4), (3,3)} is a relation on A = {1,2,3,4}.
- R^1 = R = {(1,2),(2,3),(2,4), (3,3)}
- R^2 = {(1,3), (1,4), (2,3), (3,3)}
- R^3 = {(1,3), (2,3), (3,3)}
- R^4 = {(1,3), (2,3), (3,3)}
- $R^k = R^3$, k > 3.

Theorem 1: The relation R on a set A is transitive if and only if $R^n \subseteq R$ for n = 1,2,3,... .

Number of reflexive relations

Theorem 2: The number of reflexive relations on a set A, where

| A | = n is: $2\ n(n-1)$.

Representing binary relations Using graphs

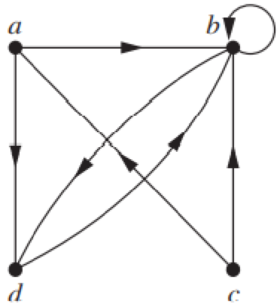
- We have shown that a relation can be represented by listing all of its ordered pairs or by using a zero–one matrix.
- We use such pictorial representations when we think of relations on a finite set as directed graphs, or digraphs.

Definition:

A **directed graph or digraph** consists of a set V of vertices (or nodes) together with a set E of ordered pairs of elements of V called edges (or arcs). The vertex a is called the initial vertex of the edge (a,b) and vertex b is the terminal vertexof this edge.

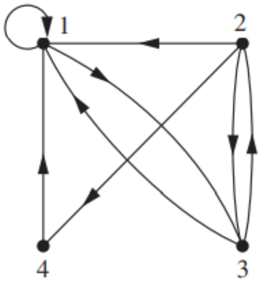
An edge of the form (a, a) is represented using an arc from the vertex a back to itself. Such an edge is called a **loop.**

Example : The directed graph with vertices a, b, c, and d, and edges (a, b), (a, d), (b, b), (b, d), (c, a), (c, b), and (d, b) is displayed in Figure down .



Example : Assume the relation R = {(1, 1), (1, 3), (2, 1), (2, 3), (2, 4), (3, 1), (3, 2), (4, 1)} on the set {1, 2, 3, 4}

The directed graph of is shown in down.



9.4 Closures of relations

- **Relations can have different properties:**
  - **reflexive,**
  - **symmetric**
  - **transitive**

- Because of that we define:
  - **symmetric closures.**
  - **reflexive closures.**
  - **transitive closures.**

Definition:

Let R be a relation on a set A. A relation S on A with property P is called **the closure of R with respect to P** if S is asubset of every relation Q ($S \subseteq Q$) with property P that containsR ($R \subseteq Q$).

Example : Let R={(1,1),(1,2),(2,1),(3,2)} on A ={1 2 3}.

- Is this relation reflexive?
- Answer: **No.** Why?
- **(2,2) and (3,3) is not in R.**

- The question is what is **the minimal relation S** $\supseteq$ R that is reflexive?
- How to make R reflexive with minimum number of additions?
- **Answer:** Add (2,2) and (3,3)
  - Then S= {(1,1),(1,2),(2,1),(3,2),(2,2),(3,3)}
  - $R \subseteq S$
  - The minimal set S $\supseteq$ R is called **the reflexive closure of R**

Definition: Reflexive closure

The set S is called **the reflexive closure of R** if it:

– contains R

– has reflexive property

– is contained in every reflexive relation Q that contains R (R $\subseteq$ Q) , that is S $\subseteq$ Q

Definition: Symmetric closure

The set S is called **the reflexive closure of R** if it can be constructed by taking the union of a relation with its inverse S = R ∪ R^{-1}

Example (a symmetric closure):

- Assume R={(1,2),(1,3), (2,2)} on A={1,2,3}.
- What is the symmetric closure S of R?
- **S = {(1,2),(1,3), (2,2)} ∪ {(2,1), (3,1)}**
  = {(1,2),(1,3), (2,2),(2,1), (3,1)}

Transitive closure

Theorem: The relation R on a set A is transitive if and only if $R^n \subseteq R$ for n = 1,2,3,... .

Example (a transitive closure):

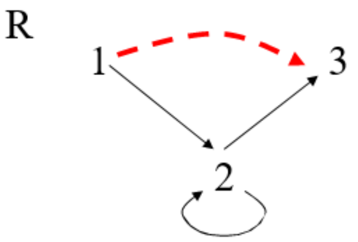
- Assume R={(1,2), (2,2), (2,3)} on A={1,2,3}.
- **Is R transitive? No.**
- **How to make it transitive?**
- **S = {(1,2), (2,2), (2,3)} ∪ {(1,3)}**
  = {(1,2), (2,2), (2,3),(1,3)}

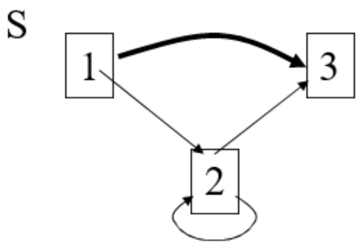
Thus S is the transitive closure of R

- We can represent the relation on the graph. Finding a transitive closure corresponds to finding all pairs of elements that are connected with a directed path (or digraph).

Example:

- Assume R={(1,2), (2,2), (2,3)} on A={1,2,3}.
- Transitive closure S = {(1,2), (2,2), (2,3),(1,3)}.





Paths in Directed Graphs

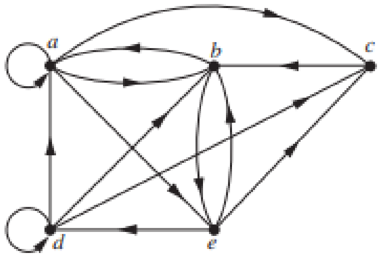
- Constructing the transitive closure of a relation is more complicated than constructing either the reflexive or symmetric closure.
- We now introduce some terminology that we will use for this purpose.

Definition: **Paths in Directed Graphs**

A path from a to b in the directed graph **G** is a sequence of edges $(x_0, x_1), (x_1, x_2), (x_2, x_3), \ldots, (x_{n-1}, x_n)$ in **G**, where n is a nonnegative integer, and x_0 = **a** and x_n = **b**, that is, a sequence of edges where the terminal vertex of an edge is the same as the initial vertex in the next edge in the path. This path is denoted by $x_0, x_1, x_2, \ldots, x_{n-1}, x_n$ and has length n. We view the empty set of edges as a path of length zero from **a to a**. A path of length $n \geq 1$ that begins and ends at the same vertex is called a circuit or **cycle.**

Note: A path in a directed graph can pass through a vertex more than once. Moreover, an edge in a directed graph can occur more than once in a path.

Example: Which of the following are paths in the directed graph shown in the Figure down: a, b, e, d; a, e, c, d, b; b, a, c, b, a, a, b; d,c; c, b, a; e, b, a, b, a, b, e? What are the lengths of those that are paths? Which of the paths in this list are circuits?



Solution:

- Because each of (a, b), (b, e), and (e, d) is an edge, a, b, e, d is a path of length three.
- Because (c, d) is not an edge, a, e, c, d, b is not a path.
- Also, b, a, c, b, a, a, b is a path of length six because (b, a), (a, c), (c, b), (b, a), (a, a), and (a, b) are all edges.
- We see that d,c is a path of length one, because (d, c) is an edge.
- Also c, b, a is a path of length two, because (c, b) and (b, a) are edges.
- All of (e, b), (b, a), (a, b), (b, a), (a, b), and (b, e) are edges, so e, b, a, b, a, b, e is a path of length six.
- The two paths b, a, c, b, a, a, b and e, b, a, b, a, b, e are circuits because they begin and end at the same vertex.
- The paths a, b, e, d; c, b, a; and d,c are not circuits.

Theorem (Path length) : Let R be a relation on a set A. There is a path of length n from a to b if and only if $(a,b) \in R^n$

Example:

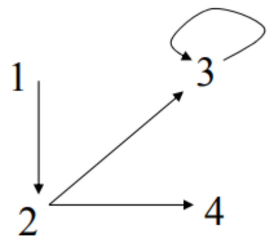
R = {(1,2),(2,3),(2,4), (3,3)} is a relation on A = {1,2,3,4}.

$R^1 = R$ = {(1,2),(2,3),(2,4), (3,3)}

R^2 = {(1,3), (1,4), (2,3), (3,3)}

What does R^2 represent? **Paths of length 2**

R^3 = {(1,3), (2,3), (3,3)} **Paths of length 3**



Definition: **Connectivity relation**

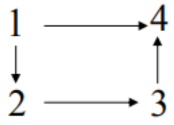
Let R be a relation on a set A. The **connectivity relation** R* consists of the pairs (a, b) such that there is a path of length at least one from a to b in R.

$$R^* = \bigcup_{k=1}^{\infty} R^k$$

Example:

A = {1,2,3,4}

R = {(1,2),(1,4),(2,3),(3,4)}



R^2 = {(1,3),(2,4)}

R^3 = {(1,4)}

$R^4 = \varnothing$

...

R* = {(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)}

Theorem: The transitive closure of a relation R **equals** the connectivity relation R*.

Theorem: Let M_R be the zero–one matrix of the relation R on a set with n elements. Then the zero–one matrix of the transitive closure R^* is $M_{R^*} = M_R \vee M^{[2]}_R \vee M^{[3]}_R \vee\cdots\vee M^{[n]}_R$.

Example: Find the zero–one matrix of the transitive closure of the relation R where

$$\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

Solution: By Theorem, it follows that the zero–one matrix of R^* is $M_{R^*} = M_R \vee M^{[2]}_R \vee M^{[3]}_R$. Because

$$\mathbf{M}_R^{[2]} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad \mathbf{M}_R^{[3]} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix},$$

it follows that

$$\mathbf{M}_{R^*} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} \vee \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \vee \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

Definition: Equivalence relation

A relation R on a set A is called an **equivalencerelation** if it is **reflexive, symmetric and transitive.**

Example: Let A = {0,1,2,3,4,5,6} and

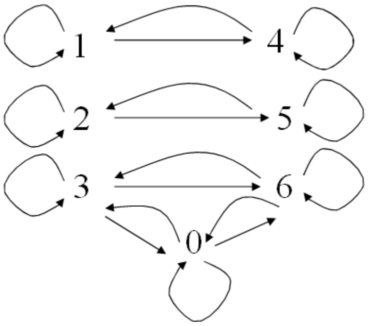
R= {(a,b)| a,b $\in$ A, a $\equiv$ b mod 3}   (a is congruent to b modulo 3)

Congruencies:

- 0 mod 3 = 0   1 mod 3 = 1   2 mod 3 = 2   3 mod 3 = 0
- 4 mod 3 = 1   5 mod 3 = 2   6 mod 3 = 0

Relation R has the following pairs:

- (0,0)   (0,3), (3,0), (0,6), (6,0)
- (3,3), (3,6) (6,3),   (1,1),(1,4), (4,1), (4,4) ,(6,6)
- (2,2), (2,5), (5,2), (5,5)



Is R reflexive? **Yes.**

Is R symmetric? **Yes.**

Is R transitive. **Yes.**

Then

R is an equivalence relation.

Ch10 Graphs

10.1 Graphs and Graph Models

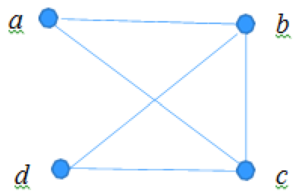
Definition:

A *graph* $G = (V, E)$ consists of a nonempty set V of *vertices* (or *nodes*) and a set E of *edges*. Each edge has either one or two vertices associated with it, called its *endpoints*. An edge issaid to *connect* its endpoints.

Remark:

The set of vertices V of a graph G may be **infinite**. A graph with an infinite vertex set or an infinite number of edges is called an **infinite graph**, and in comparison, a graph with **a finite** vertex set and a finite edge set is called **a finite graph.**

Example:

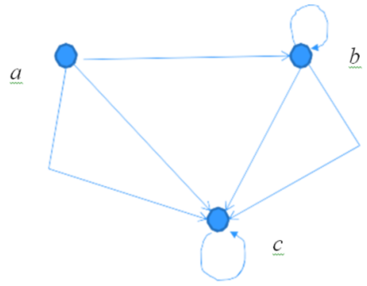


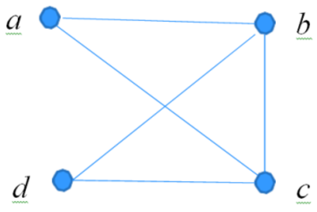
Basic types of graphs:

- **Directed graphs**

  Undirected graphs

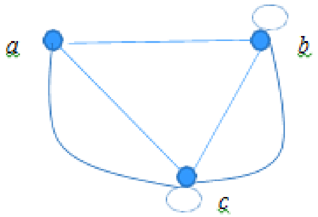
    - ○ Graphs where the end points of an edge are not ordered





Terminology

- In a ***simple graph*** each edge connects two different vertices and no two edges connect the same pair of vertices.
- ***Multigraphs*** may have multiple edges connecting the same two vertices. When *m* different edges connect the vertices *u* and *v*, wesay that {*u*,*v*} is an edge of *multiplicity m*.
- An edge that connects a vertex to itself is called a ***loop***.
- A ***pseudograph*** may include loops, as well as multiple edges connecting the same pair of vertices.

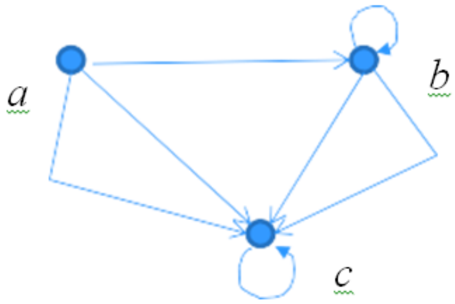


Directed graph

- A *simple directed graph* has no loops and no multiple edges.

Example:

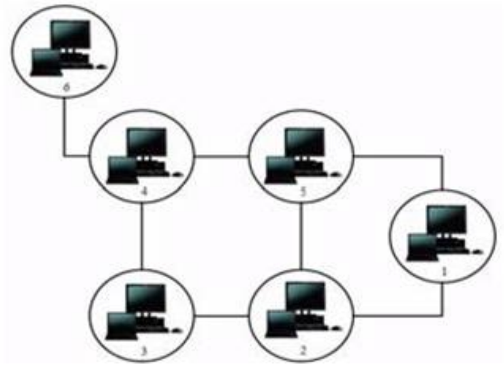
- multiplicity of (*a*,*b*) is ? 1
- and the multiplicity of (b,c) is 2



- **Graphs and graph theory can be used to model:**
  - Computer networks
  - Social networks
  - Communications networks
  - Information networks
  - Software design
  - Transportation networks
  - Biological networks

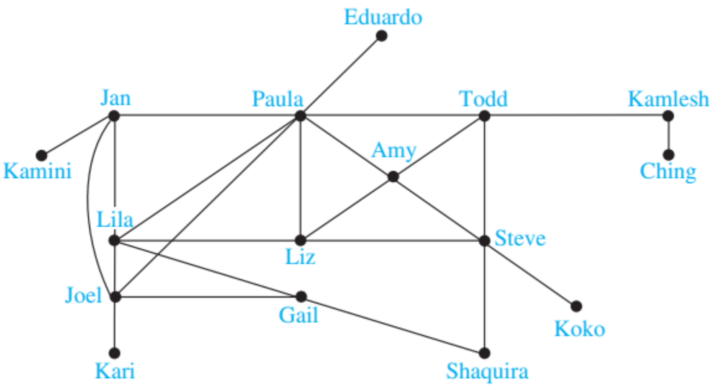
Graph models

- **Computer networks:**
  - **Nodes – computers**
  - **Edges - connections**

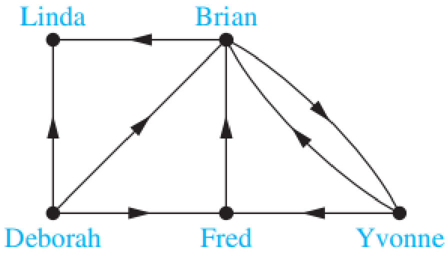


- **Social networks:**

- Graphs can be used to model social structures based on different kinds of relationships between people or groups.
- ***Social network***, vertices represent individuals or organizations and edges represent relationships between them.
- Useful graph models of social networks include:
  - ***friendship graphs*** - undirected graphs where two people are connected if they are friends (in the real world, on Facebook, or in a particular virtual world, and so on.)



- Useful graph models of social networks include:
  - ***influence graphs*** - directed graphs where there is an edge from one person to another if the first person can influence the second person



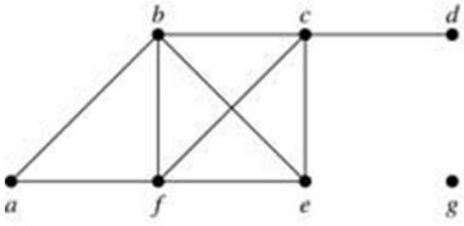
Graph characteristics: Undirected graphs

Definition 1. Two vertices u, v in an undirected graph G are called ***adjacent*** **(or *neighbors*)** in G if there is an edge e between $u$and v. Such an edge e is called *incident with* the vertices u and v and e is said to *connect* u and v.

Definition 2. The set of all neighbors of a vertex v of $G = (V, E)$, denoted by $N(v)$, is called **the *neighborhood* of *v***. If A is a subset of V, we denote by $N(A)$ the set of all vertices in G that are adjacent to at least one vertex in A.

Definition 3. The ***degree of a vertex in a undirected graph*** is the number of edges incident with it, except that a loop at a vertex contributes two to the degree of that vertex. The degree of the vertex v is denoted by deg(v).

Example: What are the degrees and neighborhoods of the vertices in the graphs G?



G

Solution:

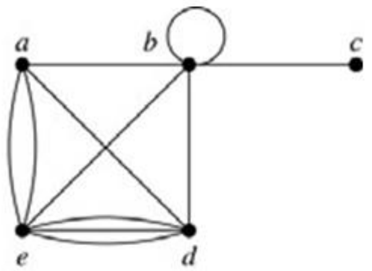
G: deg(a) = 2, deg(b) = deg(c) = deg(f) = 4, deg(d) = 1,

deg(e) = 3, deg(g) = 0.

$N(a) = \{b, f\}$, $N(b) = \{a, c, e, f\}$, $N(c) = \{b, d, e, f\}$,

$N(d) = \{c\}$, $N(e) = \{b, c, f\}$, $N(f) = \{a, b, c, e\}$, $N(g) = \varnothing$.

Example: What are the degrees and neighborhoods of thevertices in the graphs *H*?



H

Solution:

H: deg(*a*) = 4, deg(*b*) = deg(*e*) = 6, deg(*c*) = 1, deg(*d*) = 5.

N(*a*) = {*b, d, e*}, *N*(*b*) = {*a, b, c, d, e*}, *N*(*c*) = {*b*},

N(*d*) = {*a, b, e*}, *N*(*e*) = {*a, b ,d*}

Theorem 1 (*Handshaking Theorem*): If *G* = (*V*,*E*) is anundirected graph with *m* edges, then

$$2m = \sum_{v \in V} \deg(v)$$

Proof:

Each edge contributes twice to the degree count of all vertices.Hence, both the left-hand and right-hand sides of this equation equal twice the number of edges.

Theorem 2: An undirected graph has an even number of verticesof odd degree.

Proof: Let V_1 be the vertices of even degree and V_2 be the verticesof odd degree in an undirected graph *G* = (*V*, *E*) with *m* edges.

Then

$$2m = \sum_{v\in V} \deg(v) = \sum_{v\in V_1} \deg(v) + \sum_{v\in V_2} \deg(v).$$

Graph characteristics: Directed graphs

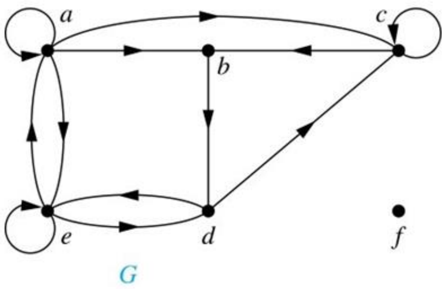
Definition: An ***directed graph*** *G* = (*V, E)* consists of *V*, a nonempty set of *vertices* (or *nodes*), and *E*, a set of *directed edges*or *arcs*. Each edge is an ordered pair of vertices. The directed edge (*u*,*v*) is said to start at *u* and end at *v*.

Definition: Let (*u*,*v*) be an edge in *G*. Then *u* is the *initial vertex* of this edge and is *adjacent to v* and *v* is the *terminal* (or *end*) *vertex* of this edge and is *adjacent from u*. The initial and terminalvertices of a loop are the same.

Definition: The *in-degree of a vertex v*, denoted *deg* $^-$(*v*), isthe number of edges which terminate at *v*. The *out-degree of v*, denoted *deg*$^+$(*v*), is the number of edges with *v* as their initial vertex. Note that a loop at a vertex contributes 1 to both the in- degree and the out-degree of the vertex.

Example: Assume graph *G:*

What are in-degrees of vertices: ?



Deg $^-$(*a*) = 2, deg $^-$(*b*) = 2,

deg $^-$(*c*) = 3,

Deg $^-$(*d*) = 2, deg $^-$(*e*) = 3, deg $^-$(*f*) = 0.

What are out-degrees of vertices: ?

deg$^+$(*a*) = 4, deg$^+$(*b*) = 1, deg$^+$(*c*) = 2,

deg$^+$(*d*) = 2, deg$^+$ (*e*) = 3, deg$^+$(*f*) = 0.

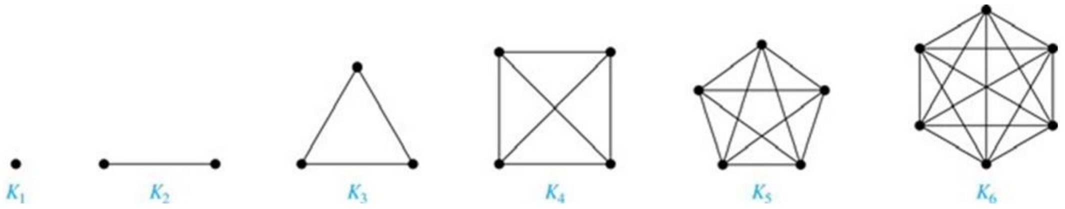
Theorem: Let $G = (V, E)$ be a graph with directed edges. Then:

$$|E| = \sum_{v \in V} deg^-(v) = \sum_{v \in V} deg^+(v).$$

Some Special Simple Graphs

Complete graphs

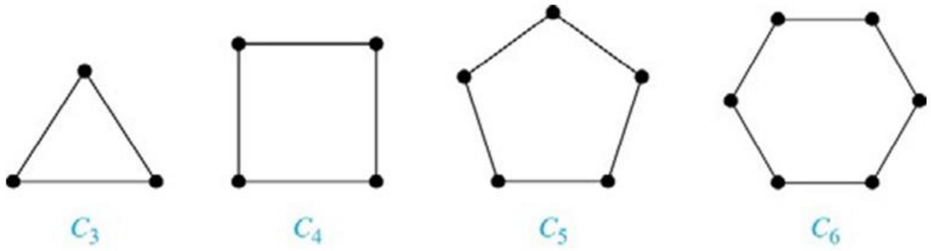
A *complete graph on n vertices*, denoted by K_n, is the simple graph that contains exactly one edge between each pair of distinctvertices.



A cycle

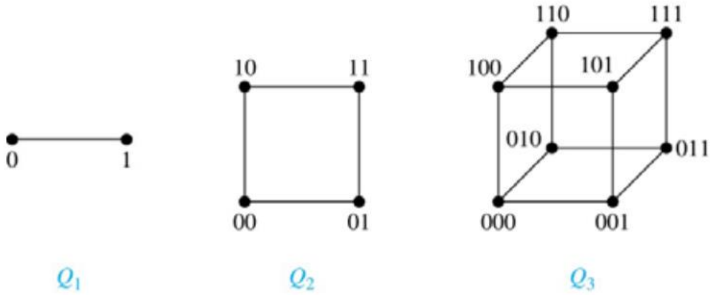
A *cycle* C_n for $n \geq 3$ consists of n vertices $v_1, v_2, \cdots, v_n$, and edges

$\{v_1, v_2\}, \{v_2, v_3\}, \cdots, \{v_{n-1}, v_n\}, \{v_n, v_1\}$.



N-dimensional hypercube

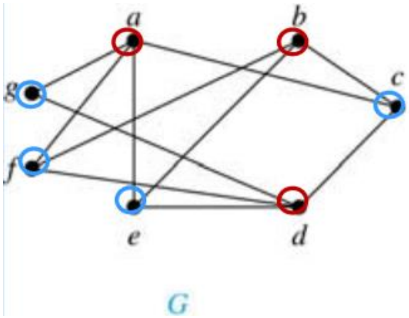
An *n-dimensional hypercube*, or *n-cube*, $\mathbf{Q_n}$, is a graph with 2^n vertices representing all bit strings of length *n*, where there is anedge between two vertices that differ in exactly one bit position.



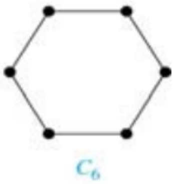
Bipartite graphs

Definition: A simple graph G is **bipartite** if V can be partitioned into two disjoint subsets V_1 and V_2 such that every edge connects avertex in V_1 and a vertex in V_2. In other words, there are no edges which connect two vertices in V_1 or in V_2.

Note: An equivalent definition of a bipartite graph is a graph where it is possible to color the vertices red or blue so that no twoadjacent vertices are the same color.



Example: Show that C_6 is bipartite.



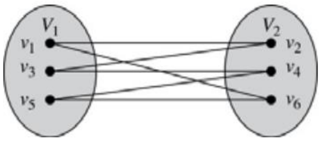
Solution:

- We can partition the vertex set into

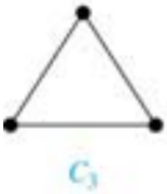
  $V_1 = \{v_1, v_3, v_5\}$ and

  $V_2 = \{v_2, v_4, v_6\}$

so that every edge of C_6 connects a vertex in V_1 and V_2 .



Example: Show that C_3 is not bipartite.



Solution:

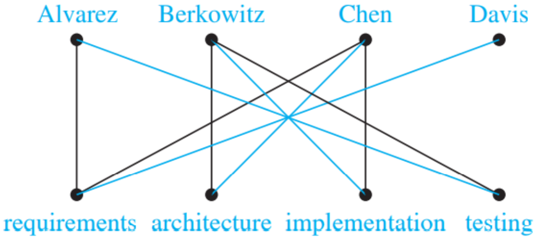
If we divide the vertex set of C_3 into two nonempty sets, one of the two must contain two vertices. But in C_3 every vertex is connected to every other vertex. Therefore, the two vertices in the same partition are connected. Hence, C_3 is not bipartite.

Bipartite graphs and matching

Bipartite graphs are used to model applications that involve **matching**

the elements of one set to elements in another, for example:

Example: *Job assignments* - vertices represent the jobs and the employees, edges link employees with those jobs they have been trained to do. A common goal is to match jobs to employees so thatthe most jobs are done.



(a)