

Discrete Structures

Mathematical Logic- Rules of Inference

Vibhavari Kamble
Asst. Prof. CoEP Pune

Rules of Inference

- ▶ ***An argument:*** a sequence of statements that end with a conclusion.
 - ▶ **argument (“valid”)** : never lead from correct statements to an incorrect conclusion.
 - ▶ **argument (“fallacies”)** : can lead from true statements to an incorrect conclusion.
- ▶ ***A logical argument*** consists of premises/hypotheses and a single proposition called the conclusion.
- ▶ ***Logical rules of inference:*** Templates for constructing valid arguments.

Valid Arguments

- Example: A logical argument

If I dance all night, then I get tired.

I danced all night.

Therefore I got tired.

- Logical representation of underlying variables:

p : I dance all night. q : I get tired.

- Logical analysis of argument:

$p \rightarrow q$ premise 1

p premise 2

$\therefore q$ conclusion

Inference Rules: General Form

- ▶ An *Inference Rule* is

A pattern establishing that if we know that a set of *premise statements of certain forms* are all true, then we can validly deduce that a certain related *conclusion* statement is true.

<i>premise 1</i>
<i>premise 2</i>
...
<hr/>
<i>∴ conclusion</i>

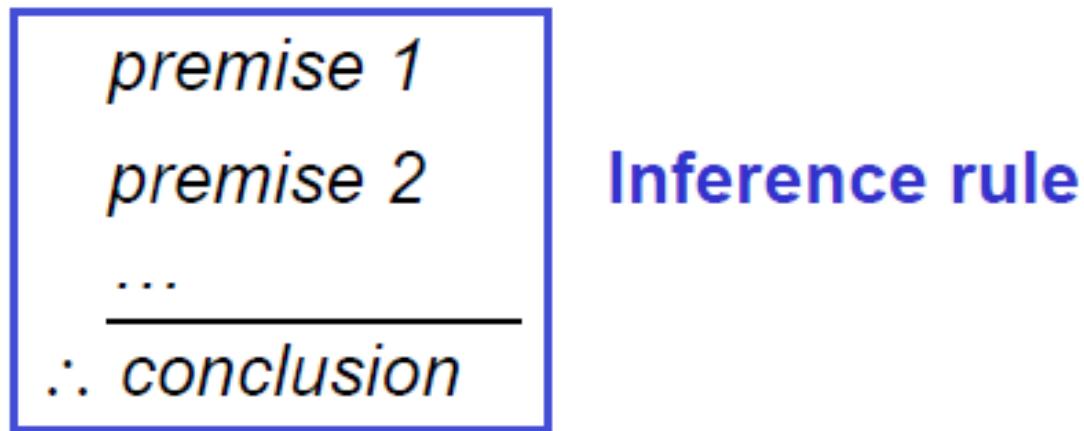
“∴” means “therefore”

Valid Arguments

- ▶ A form of logical argument is ***valid*** if whenever every premise is true, the conclusion is also true.
- ▶ A form of argument that is not valid is called a ***fallacy***.

Inference Rules Summary

- ▶ Each valid logical inference rule corresponds to an implication that is a tautology.



- ▶ Corresponding tautology:
 $((premise\ 1) \wedge (premise\ 2) \wedge \dots) \rightarrow conclusion$

Rules of inference

- ▶ Modus ponens
- ▶ Modus tollens
- ▶ Hypothetical syllogism
- ▶ Disjunctive syllogism
- ▶ Resolution
- ▶ Addition
- ▶ Simplification
- ▶ Conjunction

Modus Ponens

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

Rule of **Modus ponens**
(a.k.a. *law of detachment*)

“the mode of affirming”

$(p \wedge (p \rightarrow q)) \rightarrow q$ is a tautology

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

- ▶ Notice that the first row is the only one where premises are all true

Modus Ponens: Example

If $\left\{ \begin{array}{l} p \rightarrow q : \text{"If it snows today} \\ \quad \text{then we will go skiing"} \\ p : \text{"It is snowing today"} \end{array} \right\}$ assumed TRUE
Then $\frac{}{\therefore q} : \text{"We will go skiing"}$ is TRUE

If $\left\{ \begin{array}{l} p \rightarrow q : \text{"If } n \text{ is divisible by 3} \\ \quad \text{then } n^2 \text{ is divisible by 3"} \\ p : \text{"} n \text{ is divisible by 3"} \end{array} \right\}$ assumed TRUE
Then $\frac{}{\therefore q} : \text{"} n^2 \text{ is divisible by 3"}$ is TRUE

Modus Tollens

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

Rule of **Modus tollens**

“the mode of denying”

$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$ is a tautology

Modus Tollens: Example

■ Example

If $\left\{ \begin{array}{l} p \rightarrow q : \text{"If this jewel is really a diamond} \\ \quad \text{then it will scratch glass"} \\ \hline \neg q : \text{"The jewel doesn't scratch glass"} \end{array} \right\}$ assumed TRUE

Then $\therefore \neg p : \text{"The jewel is not a diamond"}$ is TRUE

More Inference Rules

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

Rule of **Addition**

Tautology: $p \rightarrow (p \vee q)$

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

Rule of **Simplification**

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

- $$\frac{\begin{array}{c} p \\ q \end{array}}{\therefore p \wedge q}$$

Rule of **Conjunction**

Tautology: $[(p) \wedge (q)] \rightarrow p \wedge q$

Examples

- ▶ State which rule of inference is the basis of the following arguments:
 - ▶ It is below freezing and raining now. Therefore, it is below freezing now.

Examples

- ▶ State which rule of inference is the basis of the following arguments:
 - ▶ It is below freezing and raining now. Therefore, it is below freezing now.

- ▶ p : *It is below freezing now.*
- ▶ q : *It is raining now.*
- ▶ **$(p \wedge q) \rightarrow p$ (rule of simplification)**

Quick Quiz 4.1:

- ▶ State which rule of inference is the basis of the following argument:

“It is below freezing now. Therefore, it is below freezing or raining now.”

Visit moodle to submit answer

Quick Quiz 4.1:

- ▶ State which rule of inference is the basis of the following argument:

“It is below freezing now. Therefore, it is below freezing or raining now.”

Answer:

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

This is an argument that uses **the addition rule**.

Examples

- ▶ State which rule of inference is the basis of the following arguments:
 - ▶ It is below freezing, It is raining now. Therefore, it is below freezing and raining now.

- ▶ p : *It is below freezing now.*
- ▶ q : *It is raining now.*
- ▶ $(p) \wedge (q) \rightarrow (p \wedge q)$ (*rule Conjunction*)

Hypothetical Syllogism

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

Rule of ***Hypothetical syllogism***
Tautology:

$$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$$

Example:

- ▶ State the rule of inference used in the argument:

“If it rains today, then we 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.”

“If it rains today, then we 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.”

$p \qquad q$
 r

$$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$$

Disjunctive Syllogism

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

Rule of ***Disjunctive syllogism***

Tautology: $[(p \vee q) \wedge (\neg p)] \rightarrow q$

Example

Ed's wallet is in his back pocket or it is on his desk.
Ed's wallet is not in his back pocket. Therefore, Ed's
wallet is on his desk.

Example

- Ed's wallet is in his back pocket or it is on his desk. ($p \vee q$) p q
- Ed's wallet is not in his back pocket. ($\neg p$)
- Therefore, Ed's wallet is on his desk. (q)

Resolution

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

Rule of **Resolution**
Tautology:

$$[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$$

- When $q = r$:

$$[(p \vee q) \wedge (\neg p \vee q)] \rightarrow q$$

- When $r = \mathbf{F}$:

$$[(p \vee q) \wedge (\neg p)] \rightarrow q \quad (\text{Disjunctive syllogism})$$

Resolution: Example

- ▶ Use resolution to show that the hypotheses

“Jasmine is skiing or it is not snowing” and “It is snowing or Bart is playing hockey” imply that “Jasmine is skiing or Bart is playing hockey”

“Jasmine is skiing or it is not snowing” and “It is snowing or Bart is playing hockey” imply that “Jasmine is skiing or Bart is playing hockey”

$r \quad \neg p \quad p \quad q$

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

Formal Proofs

- ▶ A formal proof of a conclusion C , *given premises*
 p_1, p_2, \dots, p_n
consists of a sequence of steps, each of which applies some inference rule to premises or previously-proven statements to yield a new true statement (the *conclusion*).
- ▶ A proof demonstrates that *if the premises are true, then the conclusion is true.*

Formal Proof Example

- ▶ Suppose we have the following premises:
“It is not sunny and it is cold.”
“We will swim only if it is sunny.”
“If we do not swim, then we will take a trip.”
“If we take a trip, then we will be home by sunset.”

- ▶ Given these premises, prove the conclusion
“We will be home by sunset” using
inference rules.

-
- ▶ **Step 1:** Identify the propositions (Let us adopt the following abbreviations)

sunny = “***It is sunny***”;

cold = “***It is cold***”;

swim = “***We will swim***”;

canoe = “***We will take a trip***”;

sunset = “***We will be home by sunset***”.

-
- ▶ **Step 2:** Identify the argument. (Build the argument form)

It is not sunny and it is cold.

We will swim only if it is sunny.

If we do not swim, then we will take a trip.

If we take a trip, then we will be home by sunset.

We will be home by sunset.

-
- ▶ **Step 2:** Identify the argument. (Build the argument form)

It is not sunny and it is cold.

We will swim only if it is sunny.

If we do not swim, then we will canoe.

If we take a trip, then we will be home by sunset.

We will be home by sunset.

$\neg \text{sunny} \wedge \text{cold}$

$\text{swim} \rightarrow \text{sunny}$

$\neg \text{swim} \rightarrow \text{canoe}$

$\text{canoe} \rightarrow \text{sunset}$

$\therefore \text{sunset}$

► **Step 3:** Verify the reasoning using the rules of inference

Step

1. $\neg \text{sunny} \wedge \text{cold}$
2. $\neg \text{sunny}$
3. $\text{swim} \rightarrow \text{sunny}$
4. $\neg \text{swim}$
5. $\neg \text{swim} \rightarrow \text{canoe}$
6. canoe
7. $\text{canoe} \rightarrow \text{sunset}$
8. sunset

Proved by

- Premise #1.
- Simplification of 1.
- Premise #2.
- Modus tollens on 2 and 3.
- Premise #3.
- Modus ponens on 4 and 5.
- Premise #4.
- Modus ponens on 6 and 7.

$$\begin{array}{c} \neg \text{sunny} \wedge \text{cold} \\ \text{swim} \rightarrow \text{sunny} \\ \neg \text{swim} \rightarrow \text{canoe} \\ \text{canoe} \rightarrow \text{sunset} \\ \hline \therefore \text{sunset} \end{array}$$

Quick Quiz 4.2:

- ▶ **True or False?**
- ▶ The premises $(p \wedge q) \vee r$ and $r \rightarrow s$ imply the conclusion $p \vee s$.
- ▶ *Visit Moodle to Submit Answer.*

Quick Quiz 4.2:

True or False?

- ▶ The premises $(p \wedge q) \vee r$ and $r \rightarrow s$ imply the conclusion $p \vee s$.

Solution: True

- ▶ rewrite the premises $(p \wedge q) \vee r$ as two clauses, $p \vee r$ and $q \vee r$.
- ▶ replace $r \rightarrow s$ by the equivalent clause $\neg r \vee s$.
- ▶ $(\neg r \vee s) \wedge (p \vee r) \wedge (q \vee r)$
- ▶ $(p \vee s) \wedge (q \vee r)$
- ▶ Using the two clauses $p \vee r$ and $\neg r \vee s$, we can use resolution to conclude $p \vee s$.

Common Fallacies

- ▶ A *fallacy* is an inference rule or other proof method that is not logically valid.
- ▶ **A fallacy may yield a false conclusion!**

- ▶ **Ex.** $((p \vee q) \wedge p) \rightarrow \sim q$ is not a tautology.
- ▶ **Fallacy of Disjunction**

-
- ▶ ***Fallacy of affirming the conclusion:***
 - ▶ “ $p \rightarrow q$ is true, and q is true, so p must be true.”
(No, because F → T is true.)

 - ▶ **Example**
 - ▶ If David Cameron (DC) is president of the US, then he is at least 40 years old. ($p \rightarrow q$)
 - ▶ DC is at least 40 years old. (q)
 - ▶ Therefore, DC is president of the US. (p)

-
- ▶ ***Fallacy of denying the hypothesis:***
 - ▶ “ $p \rightarrow q$ is true, and p is false, so q must be false.”
(No, again because **F → T is true.**)
 - ▶ **Or**
 - ▶ The proposition $((p \rightarrow q) \wedge \neg p) \rightarrow \neg q$ is not a tautology

 - ▶ **Example**
 - ▶ If a person does arithmetic well then his/her checkbook will balance. ($p \rightarrow q$)
 - ▶ I cannot do arithmetic well. ($\neg p$)
 - ▶ Therefore my checkbook does not balance. ($\neg q$)

Quick Quiz 5.1

- ▶ Is the following argument valid?

"If you do every problem in this book, then you will learn discrete mathematics." "You learned discrete mathematics." Therefore, "you did every problem in this book."

- ▶ Visit Moodle : To Submit Your Answer.

Quick Quiz 5.1

- ▶ Is the following argument valid?

"If you do every problem in this book, then you will learn discrete mathematics." "You learned discrete mathematics." Therefore, "you did every problem in this book."

- ▶ **Solution:**

Let

p : "You did every problem in this book."

q : "You learned discrete mathematics."

Argument is of the form: if $p \rightarrow q$ and q, then p.

This is an example of an incorrect argument using the **fallacy of affirming the conclusion**.

Inference Rules for Quantifiers

- $$\frac{\forall x P(x)}{\therefore P(c)}$$
 (substitute any specific member c in the domain) **Universal instantiation**
- $$\frac{P(c)}{\therefore \forall x P(x)}$$
 (for an arbitrary element c of the domain) **Universal generalization**
- $$\frac{\exists x P(x)}{\therefore P(c)}$$
 (substitute an element c for which P(c) is true) **Existential instantiation**
- $$\frac{P(c)}{\therefore \exists x P(x)}$$
 (for some element c in the domain) **Existential generalization**

Example

Show that the premises imply the conclusion

- ▶ *“Every animal has brain.” and “Human is a animal.”
Therefore, “Human has brain.”*

Example

- ▶ *Every animal has brain. Human is a animal. Therefore, Human has brain.*

- ▶ **Proof**

- ▶ Define the predicates:

$M(x)$: *x is a animal*

$L(x)$: *x has brain*

J : *Human, a member of the universe*

- ▶ The argument becomes

$$\begin{aligned} 1. \quad & \forall x [M(x) \rightarrow L(x)] \\ 2. \quad & \frac{M(J)}{\therefore L(J)} \end{aligned}$$

$$\frac{\forall x (M(x) \rightarrow L(x))}{\therefore L(J)}$$

-
- ▶ The proof is

- ▶ **Note:** Using the rules of inference requires lots of practice.
 - ▶ Try example problems in the textbook.

$$\frac{\forall x (M(x) \rightarrow L(x)) \quad M(J)}{\therefore L(J)}$$

- The proof is

1. $\forall x [M(x) \rightarrow L(x)]$

Premise 1

2. $M(J) \rightarrow L(J)$

U. I. from (1)

3. $M(J)$

Premise 2

4. $L(J)$

Modus Ponens from (2) and (3)

- **Note:** Using the rules of inference requires lots of practice.

- Try example problems in the textbook.

Combining Rules of Inference for Propositions and Quantified Statements

Universal Modus Ponens:

- ▶ If $\forall x(P(x) \rightarrow Q(x))$ is true, and if $P(a)$ is true for a particular element a in the domain of the universal quantifier, then $Q(a)$ must also be true.

$$\frac{\begin{array}{c} \forall x(P(x) \rightarrow Q(x)) \\ P(a), \text{ where } a \text{ is a particular element in the domain} \end{array}}{\therefore Q(a)}$$

EXAMPLE

- ▶ Assume that

“For all positive integers n , if n is greater than 4, then n^2 is less than 2^n ”

is true. Use universal modus ponens to show that $100^2 < 2^{100}$.

EXAMPLE

Solution:

$P(n)$: “ $n > 4$ ”

$Q(n)$: “ $n^2 < 2^n$ ”

“For all positive integers n , if n is greater than 4, then n^2 is less than 2^n ”

Represented by $\forall n(P(n) \rightarrow Q(n))$, Assumed True

- ▶ $P(100)$ is true because $100 > 4$.
- ▶ It follows by universal modus ponens that $Q(100)$ is true, namely, that $100^2 < 2^{100}$.

► Universal Modus tollens

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

$\neg Q(a)$, where a is a particular element in the domain

$$\therefore \neg P(a)$$

► Universal Modus tollens

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

$\neg Q(a)$, where a is a particular element in the domain

$$\therefore \neg P(a)$$



Discrete Structures

Introduction to Proofs



Vibhavari Kamble
Asst. Prof. CoEP Pune

Quick Quiz 5.2:

- ▶ **Correct or incorrect:**

“At least one of the 20 students in the class is intelligent. John is a student of this class. Therefore, John is intelligent.”

To submit answer visit moodle

► **Step 1:**

Separate premises from conclusion

Premises:

1. *At least one of the 20 students in the class is intelligent.*
2. *John is a student of this class.*

Conclusion:

John is intelligent.

▶ **Step 2:**

Translate the example in logic notation.

- ▶ **Premise 1:** *At least one of the 20 students in the class is intelligent.* (Let the domain = all people)

$C(x) = "x \text{ is in the class}"$

$I(x) = "x \text{ is intelligent}"$

Then Premise 1 says: $\exists x(C(x) \wedge I(x))$

- ▶ **Premise 2:** *John is a student of this class.*

Then Premise 2 says: $C(John)$

- ▶ **Conclusion:** *John is intelligent.*

And the Conclusion says: $I(John)$

► **Step 2:**

Translate the example in logic notation.

- **Premise 1:** *At least one of the 20 students in the class is intelligent.* (Let the domain = all people)

$C(x)$ = “*x is in the class*”

$I(x)$ = “*x is intelligent*”

Then Premise 1 says: $\exists x(C(x) \wedge I(x))$

- **Premise 2:** *John is a student of this class.*

Then Premise 2 says: $C(John)$

- **Conclusion:** *John is intelligent.*

And the Conclusion says: $I(John)$

$$\frac{\exists x (C(x) \wedge I(x)) \quad C(John)}{\therefore I(John)}$$

$$\begin{array}{c}
 \exists x (C(x) \wedge I(x)) \\
 C(John) \\
 \hline
 \therefore I(John)
 \end{array}$$

- ▶ No, the argument is invalid; we can disprove it with a counter-example, as follows:
- ▶ Consider a case where there is only one intelligent student A in the class, and $A \neq John$.
 - ▶ Then by existential instantiation of the premise $\exists x (C(x) \wedge I(x)) \wedge C(A) \rightarrow I(A)$ is true,
 - ▶ But the conclusion $I(John)$ is false, since A is the only intelligent student in the class, and $John \neq A$.
- ▶ Therefore, the premises do not imply the conclusion.

Proof Terminology

- ▶ A ***proof*** is a valid argument that establishes the truth of a mathematical statement
- ▶ ***Axiom (or postulate)***: a statement that is assumed to be true
- ▶ ***Theorem***
 - A statement that has been proven to be true
- ▶ ***Hypothesis, premise***
 - An assumption (often unproven) defining the structures about which we are reasoning

More Proof Terminology

- ▶ ***Lemma***

A minor theorem used as a stepping-stone to proving a major theorem.

- ▶ ***Corollary***

A minor theorem proved as an easy consequence of a major theorem.

- ▶ ***Conjecture***

A statement whose truth value has not been proven. (A conjecture may be widely believed to be true, regardless.)

Methods of Proving Theorems

Example:

To prove a theorem of the form $\forall x(P(x) \rightarrow Q(x))$

Note:

"If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$ "

really means

"For all positive real numbers x and y , if $x > y$, then $x^2 > y^2$."

Proof Methods

- ▶ For proving implications $p \rightarrow q$, we have:
- ▶ **Trivial proof:** Prove q by itself.
- ▶ **Direct proof:** Assume p is true, and prove q .
- ▶ **Indirect proof:**

Proof by Contraposition ($\neg q \rightarrow \neg p$):

Assume $\neg q$, and prove $\neg p$.

Proof by Contradiction:

Assume $p \wedge \neg q$, and show this leads to a contradiction. (i.e. prove $(p \wedge \neg q) \rightarrow F$)

- ▶ **Vacuous proof:** Prove $\neg p$ by itself.

Direct Proof Example

- ▶ Starting with the hypothesis and leading to the conclusion.
- ▶ E.g.
- ▶ **Definition:** An integer n is called odd iff $n=2k+1$ for some integer k ; n is even iff $n=2k$ for some k .
- ▶ **Theorem:** Every integer is either odd or even, but not both.
This can be proven from even simpler axioms.

► **Theorem:**

(For all integers n) *If n is odd, then n^2 is odd.*

► **Proof:** To prove $P(n) \rightarrow Q(n)$ assume $P(n)$ is true.

If n is odd, then $n = 2k + 1$ for some integer k .

Thus, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

Therefore n^2 is of the form $2j + 1$ (with j the integer $2k^2 + 2k$), thus n^2 is odd.

Quick Quiz 6.1

Let the statement be “If n is not an odd integer then square of n is not odd.”, then if $P(n)$ is “ n is an not an odd integer” and $Q(n)$ is “(square of n) is not odd.” For direct proof we should prove _____

Visit moodle to submit answer

Indirect Proof : Proof by Contraposition

- ▶ That do not start with the premises and end with the conclusion, are called **indirect proofs**.
- ▶ An extremely useful type of indirect proof is known as **proof by contraposition**.
- ▶ The conditional statement $p \rightarrow q$ *can be proved by showing that its contrapositive, $\sim q \rightarrow \sim p$, is true.*
- ▶ **Note:** we take $\neg q$ as a premise

Indirect Proof Example: Proof by Contraposition

- ▶ **Theorem: (For all integers n)**

If $3n + 2$ is odd, then n is odd.

- ▶ **Proof:**

(Contrapositive: If n is even, then $3n + 2$ is even)

Suppose that the conclusion is false, i.e., that n is even.

Then $n = 2k$ for some integer k .

Then $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$.

Thus $3n + 2$ is even, because it equals $2j$ for an integer $j = 3k + 1$. So $3n + 2$ is not odd.

We have shown that $\neg(n \text{ is odd}) \rightarrow \neg(3n + 2 \text{ is odd})$, thus its contrapositive $(3n + 2 \text{ is odd}) \rightarrow (n \text{ is odd})$ is also true. ■

Vacuous Proof Example

- ▶ Show $\neg p$ (*i.e.* p is false) to prove $p \rightarrow q$ is true.
- ▶ *E.g.*
- ▶ **Theorem:** (For all n) If n is both odd and even, then $n^2 = n + n$.



-
- **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

- ▶ Show q (*i.e.* q is true) to prove $p \rightarrow q$ is true.
- ▶ **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 hypothesis. Thus the implication is true trivially.



Proof by Contradiction

A method for proving p .

- ▶ Assume $\neg p$, and prove both q and $\neg q$ for some proposition q . (Can be anything!)
- ▶ Thus $\neg p \rightarrow (q \wedge \neg q)$
- ▶ $(q \wedge \neg q)$ is a trivial contradiction, equal to F
- ▶ Thus $\neg p \rightarrow F$, which is only true if $\neg p = F$
- ▶ Thus p is true



Rational Number

► Definition:

The real number r is rational if there exist integers p and q with $q \neq 0$ such that $r = p/q$. (p/q is in lowest terms i.e. no common factors) A real number that is not rational is called irrational.

Proof by Contradiction: Example

Theorem: $\sqrt{2}$ is irrational.

Proof by Contradiction: Example

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

Solution:

- ▶ Let p : " $\sqrt{2}$ is irrational."
- ▶ Suppose that $\sim p$ = " $\sqrt{2}$ is rational" is true. (leads to a contradiction.)
- ▶ So $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors.
- ▶ Both sides of this equation are squared $2b^2 = a^2$.
- ▶ It follows that a is even. so assume $a = 2c$
- ▶ $2b^2 = 4c^2$ this means that b^2 is even.
- ▶ our assumption of $\sim p$ leads to the contradiction , So $\sim p$ must be false.
- ▶ " $\sqrt{2}$ is irrational." is true.

Quick Quiz 6.2

A proof that $p \rightarrow q$ is true based on the fact that q is true, such proofs are known as _____

Visit moodle to submit answer

Summary: Proof by Contradiction

- ▶ Proving implication $p \rightarrow q$ by contradiction
- ▶ Assume $\neg q$, and use the premise p to arrive at a contradiction, i.e. $(\neg q \wedge p) \rightarrow F$
$$(p \rightarrow q \equiv (\neg q \wedge p) \rightarrow F)$$
- ▶ How does this relate to the proof by contraposition?
- ▶ **Proof by Contraposition ($\neg q \rightarrow \neg p$):**
Assume $\neg q$, and prove $\neg p$.

Mathematical Induction

- A powerful, rigorous technique for proving that a statement $P(n)$ is true for **every** positive integers n , no matter how large.
- Essentially a “domino effect” principle.
- Based on a predicate-logic inference rule:

$$P(1)$$

$$\forall k \geq 1 [P(k) \rightarrow P(k+1)]$$

$$\therefore \forall n \geq 1 P(n)$$

*“The First Principle
of Mathematical
Induction”*

Mathematical Induction

► PRINCIPLE OF MATHEMATICAL INDUCTION:

To prove that a statement $P(n)$ is true for all positive integers n , we complete two steps:

- **BASIS STEP:** Verify that $P(1)$ is true
- **INDUCTIVE STEP:** Show that the conditional statement $P(k) \rightarrow P(k+1)$ is true for all positive integers k

Inductive Hypothesis

Induction Example

- Show that, for $n \geq 1$

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

- Proof by induction

- $P(n)$: the sum of the first n positive integers is $n(n+1)/2$, i.e. $P(n)$ is

- **Basis step**: Let $n = 1$. The sum of the first positive integer is 1, i.e. $P(1)$ is true.

$$1 = \frac{1(1+1)}{2}$$

- **Inductive step:** Prove $\forall k \geq 1: P(k) \rightarrow P(k+1)$.
 - Inductive Hypothesis, $P(k)$:
$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}$$
- Let $k \geq 1$, assume $P(k)$, and prove $P(k+1)$, i.e.

$$\begin{aligned}
 1 + 2 + \cdots + k + (k+1) &= \frac{(k+1)[(k+1)+1]}{2} \\
 &= \frac{(k+1)(k+2)}{2}
 \end{aligned}$$


 $P(k+1)$

This is what
you have to
prove

- **Inductive step** continues... *By inductive hypothesis $P(k)$*

$$\begin{aligned}1 + 2 + \cdots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\&= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\&= \frac{k^2 + 3k + 2}{2} \\&= \frac{(k+1)(k+2)}{2}\end{aligned}$$

- Therefore, by the principle of mathematical induction $P(n)$ is true for all integers n with $n \geq 1$

Discrete Structures and Graph Theory

Computer Engineering
Semester III (Structure for Regular Students)

Sr. No.	Course Type	Course Name	Teaching Scheme			Credits
			L	T	P	
1	BSC	Ordinary Differential Equations and Multivariate Calculus	2	1	0	3
2	MLC	Professional Laws, Ethics, Values and Harmony	1	0	0	0
3	HSMC	Innovation and Creativity	1	0	0	1
4	SBC	Development Tools Laboratory	1	0	2	2
5	IFC	Feedback Control Systems	1	1	0	2
6	PCC	Data Structures and Algorithms – I	2	0	0	2
7	LC	Data Structures and Algorithms -I Laboratory	0	0	2	1
8	PCC	Digital Logic Design	3	0	0	3
9	LC	Digital Logic Design Laboratory	0	0	2	1
10	PCC	Discrete Structures and Graph Theory	2	1	0	3
11	PCC	Principles of Programming Languages	3	0	0	3
12	LC	Principles of Programming Languages Laboratory	0	0	2	1
		Total	16	3	8	22
				27		

Teaching Scheme

Lectures: 2 Hrs / Week

Tutorials: 1 hr / week

Examination Scheme:

Assignment/Quizzes : 40 marks

End Semester Exam : 60 marks

Course Outcomes

Students will be able to:

1. Explain formal logic and different proof techniques.
2. Recognize relation between different entities using sets, functions, and relations.
3. Use Chinese Remainder Theorem & the Euclidean algorithm for modular arithmetic.
4. Solve problems based on graphs, trees and related algorithms.
5. Relate, interpret and apply the concepts to various areas of computer science.

Course Content

Set Theory, Logic and Proofs : Propositions, Conditional Propositions, Logical Connectivity, Propositional calculus, predicates and Quantifiers, First order logic, Proofs: Proof Techniques, Mathematical Induction, Set, Combination of sets, Finite and Infinite sets, countable and Uncountable sets, Principle of inclusion and exclusion,

[8 Hrs]

Relations, Functions, Recurrence Relations: Definitions, Properties of Binary Relations, Equivalence Relations and partitions, Partial ordering relations and lattices, Chains and Anti chains. Theorem on chain, Warshall's Algorithm & transitive closure, Recurrence relations. Functions: Definition, Domain, Range, Image, etc. Types of functions: Surjection, Injection, Bijection, Inverse, Identity, Composition of Functions, Generating Function

[8 Hrs]

Number Theory: Basics of Modulo Arithmetic, Basic Prime Number Theory, GCD, LCM, Divisibility, Euclid's algorithm, Factorization, Congruences, inverse , multiplicative inverse, Chinese Remainder Theorem

[4 Hrs]

Counting: Basic Counting Techniques (sum, product, subtraction, division, exponent), Pigeonhole and Generalized Pigeonhole Principle with many examples, Permutations and Combinations and numerical problems, Binomial Coefficients Pascal's, Identity and Triangle

[6 Hrs]

Graphs & Trees: Basic terminology, multi graphs and weighted graphs, paths and circuits, shortest path Problems, Euler and Hamiltonian paths and circuits, factors of a graph, planar graph and Kuratowskis graph and theorem, independent sets, connectivity graph coloring. Trees, rooted trees, path length in rooted trees, binary search trees, spanning trees and, theorems on spanning trees, cut sets , circuits, minimum spanning trees, Kruskal's and Prim's algorithms for minimum spanning tree.

[8 Hrs]

Algebraic Systems: Algebraic Systems, Groups, Semi Groups, Monoids, Subgroups, Permutation Groups, Codes and Group codes, Isomorphism and Automorphisms, Homomorphism and Normal Subgroups, Ring, Field.

[6 Hrs]

Text Books

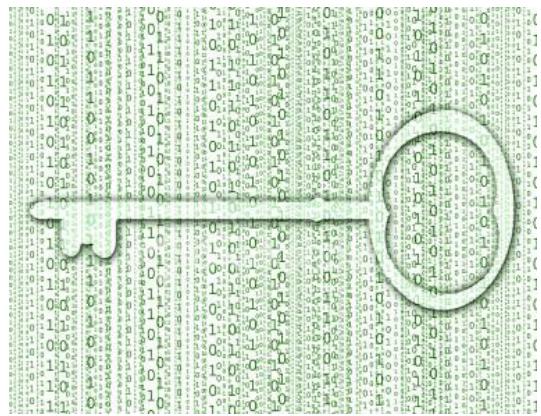
- “Discrete Mathematics and Its Applications”, Kenneth H. Rosen, 7th Edition, Tata McGraw-Hill, 2017, ISBN: 9780073383095.
- “Elements of Discrete Mathematics”, C. L. LIU, 4th Edition, Tata McGraw-Hill, 2017, ISBN-10: 1259006395 ISBN-13: 9781259006395.

Reference Books

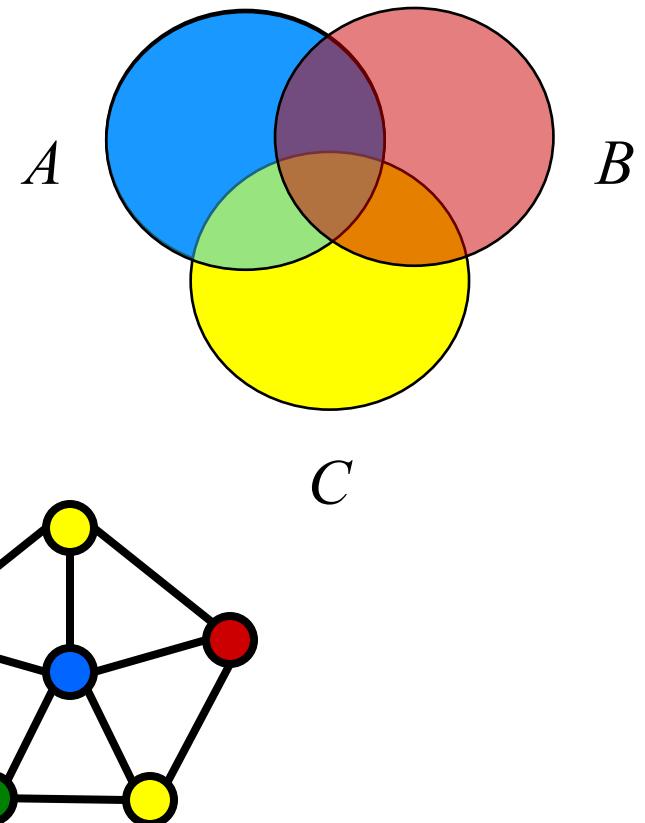
- "Discrete Mathematical Structures", G. Shanker Rao, 2nd Edition 2009, New Age International, ISBN-10: 8122426697, ISBN-13: 9788122426694
- "Discrete Mathematics", Lipschutz, Lipson, 2nd Edition, 1999, Tata McGraw-Hill, ISBN: 007463710X.
- "Graph Theory", V. K. Balakrishnan, 1st Edition, 2004, Tata McGraw-Hill, ISBN-10: 0-07-058718-3, ISBN-13: 9780070587182.
- "Discrete Mathematical Structures", B. Kolman, R. Busby and S. Ross, 4th Edition, Pearson Education, 2002, ISBN: 8178085569 ?
- "Discrete Mathematical Structures with application to Computer Science", J. Tremblay, R. Manohar, Tata McGraw-Hill, 2002, ISBN: 0070651426
- "Discrete Mathematics", R. K. Bisht, H. S. Dhami, Oxford University Press, ISBN: 9780199452798

Introduction to Discrete Mathematics

$$\frac{x_1 + x_2 + \dots + x_n}{n} \geq \sqrt[n]{x_1 \cdot x_2 \cdots x_n}$$



$$a = qb+r \quad \boxed{gcd(a,b) = gcd(b,r)}$$



Why is discrete mathematics?

Logic: artificial intelligence (AI), database, circuit design

Counting: probability, analysis of algorithm

Graph theory: computer network, data structures

Number theory: cryptography, coding theory

logic, sets, functions, relations, etc

Why is discrete mathematics?

GATE core subject

Competitive Exams

Learn Competitive Programming

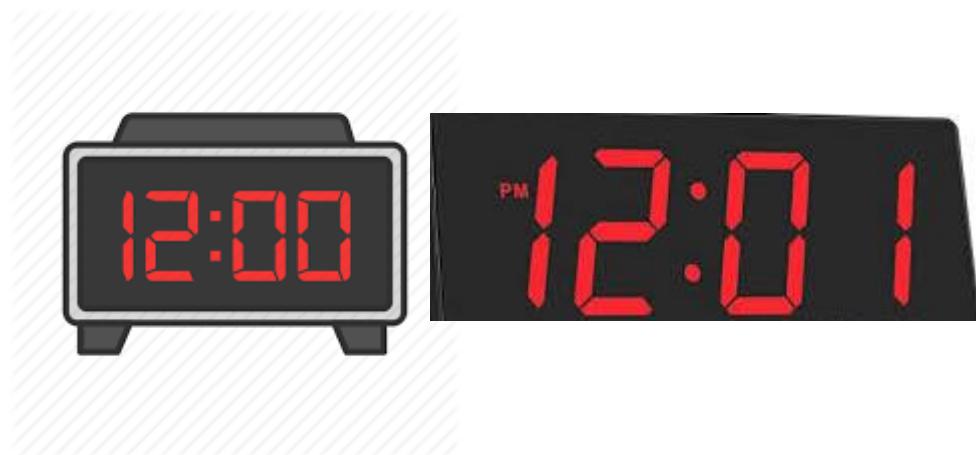
It Improves:

- Mathematical thinking
- Problem solving ability
- Foundation of all subjects in computer Engineering

What are “discrete structures” ?

“*Discrete*” - Composed of distinct, separable parts. (Opposite of *continuous*.)

discrete:continuous :: digital:analog



“*Structures*” - Objects built up from simpler objects according to some definite pattern.

“*Discrete Mathematics*” - The study of discrete, mathematical objects and structures.

Lecture 1 Link

- <https://web.microsoftstream.com/video/2c0044b2-bc32-4abe-bfa7-17ca741fa609>

Logic, Proofs and Set Theory

<https://www.youtube.com/watch?v=QmMnLxWVSGM>

CAN YOU SOLVE THIS
SIMPLE PUZZLE AND
TELL,
WHICH CAR **WAS**
STOLEN FROM THE
SHOWROOM



One day, 4 new cars went out of showroom

Blue Car

Orange Car

Red Car

Green Car



3 out of the 4 cars which went out were driven by Showroom staff

But the 4th car was driven by a thief and
was stolen

You have to Find out,
which car was stolen,
based on the clues,
which are:

- 1) Owner of the Showroom went home for Lunch in Blue car
- 2) Mechanic drove one car, but that was not the Green Car
- 3) Salesman took one car for Test Drive, but that was not Green or Orange Car

Based on these clues,
Can you tell which car
was stolen?

Lets see what is the Answer

Which car was stolen?

				
Owner				
Mechanic				
Salesman				
Thief				

Which car was stolen?

				
Owner	✓	✗	✗	✗
Mechanic	✗			
Salesman	✗			
Thief	✗			

1) Owner of the Showroom went home for Lunch in Blue car

This means, no one else took the Blue Car

Which car was stolen?

				
Owner	✓	✗	✗	✗
Mechanic	✗			✗
Salesman	✗			
Thief	✗			

- 1) Owner of the Showroom went home for Lunch in Blue car
- 2) Mechanic drove one car, but that was not the Green Car

This means, mechanic drove either Orange or Red Car

Which car was stolen?

				
Owner	✓	✗	✗	✗
Mechanic	✗			✗
Salesman	✗	✗	✓	✗
Thief	✗			

- 1) Owner of the Showroom went home for Lunch in Blue car
- 2) Mechanic drove one car, but that was not the Green Car
- 3) Salesman took one car for Test Drive, but that was not Green or Orange Car

This means, salesman drove the Red Car

Which car was stolen?

				
Owner	✓	✗	✗	✗
Mechanic	✗		✗	✗
Salesman	✗	✗	✓	✗
Thief	✗		✗	

- 1) Owner of the Showroom went home for Lunch in Blue car
- 2) Mechanic drove one car, but that was not the Green Car
- 3) Salesman took one car for Test Drive, but that was not Green or Orange Car

And no one else drove the red car

Which car was stolen?

				
Owner	✓	✗	✗	✗
Mechanic	✗	✓	✗	✗
Salesman	✗	✗	✓	✗
Thief	✗		✗	

- 1) Owner of the Showroom went home for Lunch in Blue car
- 2) Mechanic drove one car, but that was not the Green Car
- 3) Salesman took one car for Test Drive, but that was not Green or Orange Car

Which means, mechanic drove the Orange car

Which car was stolen?

				
Owner	✓	✗	✗	✗
Mechanic	✗	✓	✗	✗
Salesman	✗	✗	✓	✗
Thief	✗	✗	✗	

- 1) Owner of the Showroom went home for Lunch in Blue car
- 2) Mechanic drove one car, but that was not the Green Car
- 3) Salesman took one car for Test Drive, but that was not Green or Orange Car

And the Thief Stole the Green Car

Which car was stolen?

				
Owner	✓	✗	✗	✗
Mechanic	✗	✓	✗	✗
Salesman	✗	✗	✓	✗
Thief	✗	✗	✗	✓

GREEN CAR WAS
STOLEN



Statements/ Proposition

- Proposition or Statement or An Assertion
- Primary (Primitive, atomic) statements
- Set of Declarative sentences which cannot be further broken down into simpler sentences.
- Those who have one and only one of two possible values called “Truth Values”.
- True and False or T and F or 1 and 0
- Two-valued logic
- Some statements can be assertion but not the propositions
 - Ex. “This statement is false”

Statement (Proposition)

A *Statement* is a sentence that is either **True** or **False**

Examples: $2 + 2 = 4$ True

$3 \times 3 = 8$ False

787009911 is a prime

Non-examples: $x+y>0$

$$x^2+y^2=z^2$$

They are true for some values of x and y
but are false for some other values of x and y.

The Statement/Proposition Game

- “Elephants are bigger than ant.”

Is this a proposition? yes

**What is the truth value
of the proposition?** true

The Statement/Proposition Game

- “ $520 < 111$ ”

Is this a proposition? yes

**What is the truth value
of the proposition?** false

The Statement/Proposition Game

- “Please do not fall asleep.”

Is this a statement? no

It's a request.

Is this a proposition? no

Only statements can be propositions.

Examples of statements/ Propositions

All the following declarative sentences are propositions.

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

Propositions 1 and 3 are **true**, whereas 2 and 4 are **false**.

Examples

- Consider the following sentences.
 1. What time is it?
 2. Read this carefully.
 3. $x + 1 = 2$.
 4. $x + y = z$.

Sentences 1 and 2 are **not propositions** because they are not declarative sentences.

Sentences 3 and 4 are **not propositions** because they are neither true nor false.

Note that each of sentences 3 and 4 can be turned into a proposition if we assign values to the variables

Class Assignment

- Which of these sentences are propositions? What are the truth values of those that are propositions?
 - a) Boston is the capital of Massachusetts.
 - b) Miami is the capital of Florida.
 - c) $2 + 3 = 5$.
 - d) $5 + 7 = 10$.
 - e) $x + 2 = 11$.
 - f) Answer this question.
 - g) Do not pass go.
 - h) What time is it?
 - i) There are no black flies in Maine.
 - j) $4 + x = 5$.
 - k) The moon is made of green cheese.
 - l) $2n \geq 100$

Class Assignment

- Which of these sentences are propositions? What are the truth values of those that are propositions?
 - a) Boston is the capital of Massachusetts. T
 - b) Miami is the capital of Florida.
 - c) $2 + 3 = 5$. T
 - d) $5 + 7 = 10$. F
 - e) $x + 2 = 11$.
 - f) Answer this question.
 - g) Do not pass go.
 - h) What time is it?
 - i) $4 + x = 5$.
 - j) The moon is made of green cheese. F
 - k) $2n \geq 100$

Lecture 2

- <https://web.microsoftstream.com/video/2d775ffa-9508-4141-a3af-08b35c8d8073>

Operators/ Connectives

- An *operator* or *connective* combines one or more *operand* expressions into a larger expression.
- Two types of declarative sentences
- First is Primitive or primary or atomic statement
- Denoted by letters A,B,C.....P,Q,R...or a,b,c,...p,q,r...
 - P: London is capital of India.
 - A:Ram is poor.
- Second types are obtained from primitives using **connectives and parenthesis**, Called molecular or compound statements
- Like statements connective also denoted by **symbol**

Examples

e.g.

1. India is country and Mumbai is capital of India.

P:India is country

Q:Mumbai is capital of India.

P and Q $P \wedge Q$

2. Ram is poor but he is clever.

A: Ram is poor.

B: Ram is clever.

A and B

Connectives

1. Negation (Not)
2. Conjunction (and)
3. Disjunction (or)
4. Conditional (if...then) /implication
5. Bi-conditional (if and only if)

Connectives' Symbols

<u>Formal Name</u>	<u>Nickname</u>	<u>Property</u>	<u>Symbol</u>
Negation operator	NOT	Unary	¬
Conjunction operator	AND	Binary	∧
Disjunction operator	OR	Binary	∨
Exclusive-OR operator	XOR	Binary	⊕
Implication operator	IMPLIES	Binary	→
Biconditional operator	IFF	Binary	↔

Lecture 3

- <https://web.microsoftstream.com/video/eaf401a0-8259-4d61-af55-87efd46b1b92>
- <https://web.microsoftstream.com/video/6ef37cbd-170d-440c-ac61-cfe331ac5816>

Discrete Structures and Graph Theory

Connectives

1. Negation (Not)
2. Conjunction (and)
3. Disjunction (or)
4. Conditional (if...then) /implication
5. Bi-conditional (if and only if)

Negation (NOT)

- Statements Formed by introducing “not” word
- “P” is Statement then negation of p is written as “not p“ or It is not case that P.
- $\neg p$
- Unary Connective
- If P is true then $\neg p$ is false and vice versa.

P	$\neg P$
T	F
F	T

P:London is a city.

Then

¬ p: London is not a city.

OR

¬ p: It is not the case that London is a city.

Q: I went to my class yesterday

Then

¬ Q:I did not go to my class yesterday

Conjunction (and)

- Statements Formed by introducing “**and**” word
- Binary Connective
- Used to combine two or more statements.
- Denote by \wedge
- If both the statements are true then $P \wedge Q$ is true otherwise false.

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P:London is a capital of India.

Q: India is country.

London is a capital of India **and** India is country.

P \wedge Q

Disjunction (OR)

- Statements Formed by introducing “OR” word
- Binary Connective
- Denote by \vee
- If one statement is true then $p \vee Q$ is true otherwise false.

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

P:London is a capital of India.

Q: India is country.

London is a capital of India **or** India is country.

$P \vee Q$

Conditional (if..then)

- Statements Formed by introducing “if...then” word
- Binary Connective
- Denote by →
- If First statement is true and second statement is false then $P \rightarrow Q$ is false otherwise true.

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

“If elephants were red, then they could hide in cherry trees.”.

$$P \rightarrow Q$$

P is known as Antecedent

Q is known as consequent

For $Q \rightarrow P$, vice versa

Implication

- If you study regularly you then you will get grade ‘A’

Case 1 : You did regular study , you got A grade.

$(P \rightarrow Q)$: True

Case 2: You did regular study ,by chance you didn't get grade A. $(P \rightarrow Q)$: False

Case 3: You didn't study regularly, you may get grade A. $(P \rightarrow Q)$: True

Case 4: You didn't study regularly, you didn't get grade A. $(P \rightarrow Q)$: True

Some reading for P->Q

- “ p implies q ”
 - “if p , then q ”
 - “if p , q ”
 - “when p , q ”
 - “whenever p , q ”
 - “ q if p ”
 - “ q when p ”
 - “ q whenever p ”
 - “ p only if q ”
 - “ p is sufficient for q ”
 - “ q is necessary for p ”
 - “ q follows from p ”
 - “ q is implied by p ”
- We will see some equivalent logic expressions later.

Bi-conditional (if and only if)

- **Statements Formed by introducing “if and only if ” word**
- **Binary Connective**
- Denote by \leftrightarrow
- If both the statement has same truth value then $p \leftrightarrow Q$ is true otherwise false.

P	Q	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

“ $x < y$ if and only if $y > x$. ”

$$P \leftrightarrow Q$$

EX-OR (Either-Or)

- Statement formed by “Either Or” word.
- Exclusive Or
- $P \times Q$ proposition will be true, if exactly one of two propositions of both is true.
Otherwise false

P	Q	$P \oplus Q$
T	T	F
T	F	T
F	T	T
F	F	F

Inclusive or OR Exclusive or

- In order to get a job in this multinational company , experience with C++ **or** Java is mandatory.

Inclusive or OR Exclusive or

- In order to get a job in this multinational company , experience with C++ **or** Java is mandatory.



Inclusive OR

Disjunction

Inclusive or OR Exclusive or

- “When you buy a mobile of xyz company, you get Rs.500 cashback or a mobile cover of worth Rs.500.”

Inclusive or OR Exclusive or

- “When you buy a mobile of xyz company, you get Rs.500 cashback **or** a mobile cover of worth Rs.500.”

Exclusive OR



Statement Formula and Truth Table

- Atomic statements/proposition
- Compound statements/proposition
 - $\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$, $\neg(P \wedge Q)$, $\neg(P \wedge Q)$
- Statement formula
- Truth Table
- 2^n where n is number of distinct statement variable
- $P \wedge \neg P$
 - 2 rows, n=1, 2^1
- $(P \wedge Q)$
 - 4 rows, n=2, 2^2

- Statements and operators (Connectives and parenthesis) can be combined in any way to form new statements.
- $(\neg P) \vee (\neg Q)$

P	Q			
T	T			
T	F			
F	T			
F	F			

- Statements and operators can be combined in any way to form new statements.
- $(\neg P) \vee (\neg Q)$

P	Q	$\neg P$		
T	T	F		
T	F	F		
F	T	T		
F	F	T		

- Statements and operators can be combined in any way to form new statements.
- $(\neg P) \vee (\neg Q)$

P	Q	$\neg P$	$\neg Q$	
T	T	F	F	
T	F	F	T	
F	T	T	F	
F	F	T	T	

- Statements and operators can be combined in any way to form new statements.
- $(\neg P) \vee (\neg Q)$

P	Q	$\neg P$	$\neg Q$	$(\neg P) \vee (\neg Q)$
T	T	F	F	
T	F	F	T	
F	T	T	F	
F	F	T	T	

- Statements and operators can be combined in any way to form new statements.
- $(\neg P) \vee (\neg Q)$

P	Q	$\neg P$	$\neg Q$	$(\neg P) \vee (\neg Q)$
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

$$\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$$

P	Q		
T	T		
T	F		
F	T		
F	F		

$$\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$$

P	Q	$\neg P$	$\neg Q$
T	T	F	F
T	F	F	T
F	T	T	F
F	F	T	T

$$\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$$

P	Q	$\neg P$	$\neg Q$
T	T	F	F
T	F	F	T
F	T	T	F
F	F	T	T

$(P \wedge Q)$			
T			
T			
T			
F			

$$\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$$

P	Q	$\neg P$	$\neg Q$
T	T	F	F
T	F	F	T
F	T	T	F
F	F	T	T

$(P \wedge Q)$	$\neg(P \wedge Q)$		
T	F		
T	F		
T	F		
F	T		

$$\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$$

P	Q	$\neg P$	$\neg Q$
T	T	F	F
T	F	F	T
F	T	T	F
F	F	T	T

$(P \wedge Q)$	$\neg(P \wedge Q)$	$(\neg P) \vee (\neg Q)$	
T	F	F	
T	F	T	
T	F	T	
F	T	T	

$$\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$$

P	Q	$\neg P$	$\neg Q$
T	T	F	F
T	F	F	T
F	T	T	F
F	F	T	T

$(P \wedge Q)$	$\neg(P \wedge Q)$	$(\neg P) \vee (\neg Q)$	$\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$
T	F	F	T
F	T	T	T
F	T	T	T
F	T	T	T

$$\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$$

P	Q	$\neg P$	$\neg Q$
T	T	F	F
T	F	F	T
F	T	T	F
F	F	T	T

$(P \wedge Q)$	$\neg(P \wedge Q)$	$(\neg P) \vee (\neg Q)$	$\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$
T	F	F	T
F	T	T	T
F	T	T	T
F	T	T	T

Example

- Using the statements:

R:Mark is Rich.

H:Mark is happy

- Write the following statements in symbolic form:

- (a) Mark is poor but happy.

$\neg R \wedge H$

- (b) Mark is rich or unhappy;

$R \vee \neg H$

- (c) Mark is neither rich nor happy.

$\neg R \wedge \neg H$

- (d) Mark is poor or he is both rich and unhappy.

$\neg R \vee (R \wedge \neg H)$

Example

- Let p be "It is cold" and let q be "It is raining". Give a simple **verbal sentence** which describes each of the following statements:
 - (a) $\neg p$; (b) $p \wedge q$; (c) $p \vee q$; (d) $q \vee \neg p$.
 - (a) $\neg p$;
It is not cold.
 - (b) $p \wedge q$;
It is cold and raining.
 - (c) $p \vee q$;
It is cold or it is raining
 - (d) $q \vee \neg p$.
It is raining or it is not cold.

Example 1.17 There are two restaurants next to each other. One has a sign that says, “Good food is not cheap,” and the other has a sign that says, “Cheap food is not good.” Are the signs saying the same thing?

Using the statements:

P:Food is good.

H:Food is cheap.

Good food is not cheap.

$$P \rightarrow \neg H$$

Cheap food is not good.

$$H \rightarrow \neg P$$

$$H \rightarrow \neg P$$

P	H	$\neg P$	$\neg H$	$P \rightarrow \neg H$	$H \rightarrow \neg P$
T	T	F	F	F	F
T	F	F	T	T	T
F	T	T	F	T	T
F	F	T	T	T	T

WFF (well formed formula)

- Now consider the proposition : $P \vee \sim Q \rightarrow P \wedge R$

Trying to construct a truth table for this is quite confusing. Which is to be assumed?

$$(P \vee \sim Q) \rightarrow (P \wedge R) \text{ or } P \vee (\sim Q \rightarrow P) \wedge R$$

Which part is calculated first?

for such cases we have order of precedence for these operators.

WFF (well formed formula)

- A statement formula is said to be WFF if it has :
 1. Every Atomic statement is wff
 2. If P is wff then $\sim p$ is also wff
 3. If P and Q are wff then $(P \wedge Q)$, $(P \vee Q)$, and $(P \rightarrow Q)$ are wff
 4. Nothing else is wff

For example: $((P \wedge Q) \vee R)$ is wff w, where as $P \vee Q \wedge R$ is not a wff

Precedence of the operators

- \sim
- \wedge
- \vee, \oplus
- $\cdot \rightarrow$
- \longleftrightarrow

For example ,

$\sim P \wedge Q \rightarrow R \vee Q$ is not a wff.

can be converted to wff by using rules of precedence as $((\sim P) \wedge Q) \rightarrow (R \vee Q)$

Equivalent Statements

- If truth values of statement formula/proposition A is equal to the truth values of statement formula/proposition B for every possible truth values then A and B are logically equivalent to each other.

P	Q	$\neg P$	$\neg Q$	$\neg(P \wedge Q)$	$(\neg P) \vee (\neg Q)$
T	T	F	F	F	F
T	F	F	T	T	T
F	T	T	F	T	T
F	F	T	T	T	T

Denoted by symbol \Leftrightarrow

- Let P be "Roses are red" and Q be "Violets are blue." Let S be the statement:
"It is not true that roses are red and violets are blue."

- Then S can be written in the form $\neg(p \wedge q)$.
- Accordingly, S has the same meaning as the statement:

"Roses are not red, or violets are not blue."

Then S can be written in the form $\neg p \vee \neg q$.

However, as noted above, $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$.

Equivalent Statements

- The statements $\neg(P \wedge Q)$ and $(\neg P) \vee (\neg Q)$ are logically equivalent, since $\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$ is always true.

P	Q	$\neg P$	$\neg Q$	$\neg(P \wedge Q)$	$(\neg P) \vee (\neg Q)$	$\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$
T	T	F	F	F	F	T
T	F	F	T	T	T	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

Convert the following English statements in symbolic form.

- You can access the internet from campus if you are computer science major or you are not a freshman.

Solution: P: You can access the internet from campus.

Q: you are computer major.

R: you are a freshman.

$$P \rightarrow (Q \vee \neg R)$$

- You can ride on roller coaster if you are under 4 feet tall unless you are older than 16 years old.

Solution :

P: You can ride on roller coaster

Q: You are under 4 feet

R: You are older than 16 years old.

$(Q \vee \neg R) \rightarrow P$

Logical Equivalence

The easiest way to check for logical equivalence is to see if the truth tables of both variants have *identical last columns*:

p	q	$p \rightarrow q$

p	q	$\neg q$	$\neg p$	$\neg q \rightarrow \neg p$

Logical Equivalence

The easiest way to check for logical equivalence is to see if the truth tables of both variants have *identical last columns*:

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

p	q	$\neg q$	$\neg p$	$\neg q \rightarrow \neg p$

Logical Equivalence

The easiest way to check for logical equivalence is to see if the truth tables of both variants have *identical last columns*:

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

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

Logical Equivalence

The easiest way to check for logical equivalence is to see if the truth tables of both variants have *identical last columns*:

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

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

Logical Equivalence

The easiest way to check for logical equivalence is to see if the truth tables of both variants have *identical last columns*:

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

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

Logical Equivalence

The easiest way to check for logical equivalence is to see if the truth tables of both variants have *identical last columns*:

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

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

Exercises

- Prove that:

$$1) \ (P \rightarrow Q) \Leftrightarrow \neg P \vee Q$$

$$2) P \rightarrow (Q \rightarrow R) \Leftrightarrow (P \wedge Q) \rightarrow R.$$

Tautologies and Contradictions

- Some propositions P contain only T in the last column of their truth tables or, in other words, they are true for any truth values of their variables. Such propositions are called *tautologies*. A tautology is a statement that is always true.

Examples:

- $R \vee (\neg R)$

$$\forall \neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$$

- If $S \rightarrow T$ is a tautology, we write $S \Rightarrow T$.
- If $S \leftrightarrow T$ is a tautology, we write $S \Leftrightarrow T$.

$$\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$$

P	Q	$\neg P$	$\neg Q$
T	T	F	F
T	F	F	T
F	T	T	F
F	F	T	T

$(P \wedge Q)$	$\neg(P \wedge Q)$	$(\neg P) \vee (\neg Q)$	$\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$
T	F	F	T
F	T	T	T
F	T	T	T
F	T	T	T

Tautology by truth table

p	q	$\neg p$	$p \vee q$	$\neg p \wedge (p \vee q)$	$[\neg p \wedge (p \vee q)] \rightarrow q$
T	T				
T	F				
F	T				
F	F				

Tautology by truth table

p	q	$\neg p$	$p \vee q$	$\neg p \wedge (p \vee q)$	$[\neg p \wedge (p \vee q)] \rightarrow q$
T	T	F			
T	F	F			
F	T	T			
F	F	T			

Tautology by truth table

p	q	$\neg p$	$p \vee q$	$\neg p \wedge (p \vee q)$	$[\neg p \wedge (p \vee q)] \rightarrow q$
T	T	F	T		
T	F	F	T		
F	T	T	T		
F	F	T	F		

Tautology by truth table

p	q	$\neg p$	$p \vee q$	$\neg p \wedge (p \vee q)$	$[\neg p \wedge (p \vee q)] \rightarrow q$
T	T	F	T	F	
T	F	F	T	F	
F	T	T	T	T	
F	F	T	F	F	

Tautology by truth table

p	q	$\neg p$	$p \vee q$	$\neg p \wedge (p \vee q)$	$[\neg p \wedge (p \vee q)] \rightarrow q$
T	T	F	T	F	T
T	F	F	T	F	T
F	T	T	T	T	T
F	F	T	F	F	T

Tautologies and Contradictions

- a proposition P is called a **contradiction** if it contains only **F** in the **last column** of its truth table or, in other words, if it is false for any truth values of its variables.
- A contradiction is a statement that is always false.

Examples:

- $R \wedge \neg R$
- $\forall x \neg(\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q))$
- The negation of any tautology is a contradiction, and the negation of any contradiction is a tautology.

- Two way to finding the Equivalences,
Tautology and Contradiction
- Truth Table
- Without Truth Table Using Substitution (by
formulas)

P	Q	$\neg P$	$\neg Q$	$\neg P \vee Q$	$P \rightarrow Q$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Logical Equivalences

- Identity Laws: $p \wedge T \Leftrightarrow p$ and $p \vee F \Leftrightarrow p$.
- Domination Laws: $p \vee T \Leftrightarrow T$ and $p \wedge F \Leftrightarrow F$.
- Idempotent Laws: $p \wedge p \Leftrightarrow p$ and $p \vee p \Leftrightarrow p$.
- Double Negation Law: $\neg(\neg p) \Leftrightarrow p$.
- Commutative Laws:
 - $(p \vee q) \Leftrightarrow (q \vee p)$ and $(p \wedge q) \Leftrightarrow (q \wedge p)$.
- Associative Laws: $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$
 - and $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$.

Logical Equivalences

- Distributive Laws:
 - $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ and
 - $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r).$
- DeMorgan's Laws:
 - $\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$ and
 - $\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q).$
- Absorption Laws:
 - $p \vee (p \wedge q) \Leftrightarrow p$ and $p \wedge (p \vee q) \Leftrightarrow p.$
- Negation Laws: $p \vee \neg p \Leftrightarrow T$ and $p \wedge \neg p \Leftrightarrow F.$

Logical Equivalences for Implication

$$p \rightarrow q \equiv \neg p \vee q$$

$$p \rightarrow q \equiv \neg q \rightarrow \neg p$$

$$p \vee q \equiv \neg p \rightarrow q$$

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

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

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

$$(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$$

$$(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$$

$$(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$$

Logical Equivalences for Double Implication

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

$$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$$

$$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$$

$$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$$

Substitution instance

- A formula A is called substitution instance of formula B if A can be obtained from B by substituting formulas for some variable of B.

Examples:

- $B:P \rightarrow (J \wedge P)$
- If P be $R \leftrightarrow S$
- $A:(R \leftrightarrow S) \rightarrow (J \wedge (R \leftrightarrow S))$
- As like we can substitute the formula with another formula if both have same truth values
 - $(R \rightarrow S) \wedge (R \leftrightarrow S)$
 - $(\neg R \vee S) \wedge (R \leftrightarrow S)$
- Equivalent formula can be substitute for each other.

- Prove that $P \rightarrow (Q \rightarrow R) \Leftrightarrow (P \wedge Q) \rightarrow R$.
- $P \rightarrow (Q \rightarrow R) \Leftrightarrow P \rightarrow (\neg Q \vee R)$ **implication law**
 $\Leftrightarrow \neg P \vee (\neg Q \vee R)$..**implication law**
 $\Leftrightarrow (\neg P \vee \neg Q) \vee R$...**Associative law**
 $\Leftrightarrow \neg(P \wedge Q) \vee R$...**Associative law**
 $\Leftrightarrow (P \wedge Q) \rightarrow R$.

Prove: $(p \wedge \neg q) \vee q \Leftrightarrow p \vee q$

$(p \wedge \neg q) \vee q$ Left-Hand Statement

$\Leftrightarrow q \vee (p \wedge \neg q)$ Commutative

$\Leftrightarrow (q \vee p) \wedge (q \vee \neg q)$ Distributive

$\Leftrightarrow (q \vee p) \wedge T$ Or Tautology

$\Leftrightarrow q \vee p$ Identity

$\Leftrightarrow p \vee q$ Commutative

Prove: $(p \wedge \neg q) \vee q \Leftrightarrow p \vee q$

$$(p \wedge \neg q) \vee q \quad \text{Left-Hand Statement}$$

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

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

Why did we need this step?

Prove: $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$

$$p \rightarrow q$$

Contrapositive

$$\Leftrightarrow \neg p \vee q \quad \text{Implication Equivalence}$$

$$\Leftrightarrow q \vee \neg p \quad \text{Commutative}$$

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

$$\Leftrightarrow \neg q \rightarrow \neg p \quad \text{Implication Equivalence}$$

If $p \rightarrow q$ is a statement then $q \rightarrow p$ is called converse.

$\neg p \rightarrow \neg q$ is inverse and

$\neg q \rightarrow \neg p$ is contrapositive.

Prove: $p \rightarrow p \vee q$ is a tautology

Must show that the statement is true for any value of p,q.

$$p \rightarrow p \vee q$$

$$\Leftrightarrow \neg p \vee (p \vee q) \quad \text{Implication Equivalence}$$

$$\Leftrightarrow (\neg p \vee p) \vee q \quad \text{Associative}$$

$$\Leftrightarrow (p \vee \neg p) \vee q \quad \text{Commutative}$$

$$\Leftrightarrow T \vee q \quad \text{Or Tautology}$$

$$\Leftrightarrow q \vee T \quad \text{Commutative}$$

$$\Leftrightarrow T \quad \text{Domination}$$

This tautology is called the addition rule of inference.

Predicates & Quantifiers

Universal and Existential

Predicate Logic

- ◆ A predicate is an expression of one or more variables defined on some specific **domain**. A predicate with variables can be made a proposition by either assigning a value to the variable or by quantifying the variable.
- ◆ The following are some examples of predicates –
 - Let $E(x, y)$ denote " $x = y$ "
 - Let $X(a, b, c)$ denote " $a + b + c = 0$ "
 - Let $M(x, y)$ denote " x is married to y "
 - Let $P(x)$ denote “ x is greater than 3”
 - ◆ In last statement first part variable x ,is the subject of the statement, the second part is predicate “is greater than 3”, $P(x)$ is a propositional function P at x .

Example

- ◆ Let $P(x)$ is $x > 3$ what are the truth values for $P(2)$ and $P(4)$? Unary
- ◆ Let $Q(x,y)$ denote “ $x = y + 3$ ” what are the truth values for $Q(1,2)$ and $Q(3,0)$? Binary
- ◆ Let $R(x,y,z)$ denote “ $x + y = z$ ” what are the truth values for $R(1,2,3)$ & $R(0,0,1)$?
- ◆ Similarly for $P(x_1, x_2, \dots, x_n)$ can be a value for n tuple, and P is also known as Predicate. N-ary predicate

Example

- ◆ Let $P(x; y; z)$ denote that $x + y = z$ and U (Universe of Discourse) be the integers for all three variables.
 - $P(-4; 6; 2)$ is true.
 - $P(5; 2; 10)$ is false.
 - $P(5; x; 7)$ is not a proposition.

Quantifiers

- ◆ We need quantifiers to formally express the meaning of the words “all” and “some”.
- ◆ The two most important quantifiers are:
 - Universal quantifier, “For all”. Symbol: \forall
 - Existential quantifier, “There exists”. Symbol: \exists
- ◆ $\forall x P(x)$ asserts that $P(x)$ is true for **every x in the domain**.
- ◆ $\exists x P(x)$ asserts that $P(x)$ is true for **some x in the domain**.
- ◆ The quantifiers are said to bind the variable x in these expressions.
- ◆ Variables in the scope of some quantifier are called **bound variables**. All other variables in the expression are called **free variables**.
- ◆ A propositional function that does not contain any free variables is a proposition and has a truth value.

Quantifiers

- ◆ The variable of predicates is quantified by quantifiers. There are two types of quantifier in predicate logic –
 - Universal Quantifier and
 - Existential Quantifier.

Universal Quantifier

- ◆ Universal quantifier states that the statements within its scope are true for every value of the specific variable. It is denoted by the symbol \forall
- ◆ $\forall xP(x)$ is read as for every value of x , $P(x)$ is true.
- ◆ **Example –**
 - "Man is mortal" can be transformed into the propositional form $\forall xP(x)$
 - where $P(x)$ is the predicate which denotes x is mortal and the universe of discourse is all men.

Existential Quantifier

- ◆ Existential quantifier states that the statements within its scope are true for some values of the specific variable. It is denoted by the symbol \exists
- ◆ $\exists xP(x)$ is read as for some values of x , $P(x)$ is true.
 - **Example** – "Some people are dishonest" can be transformed into the propositional form $\exists xP(x)$
 - where $P(x)$ is the predicate which denotes x is dishonest and the universe of discourse is some people.

Uniqueness Quantifier

- $\exists ! x P(x)$ means that there exists one and only one x in the domain such that $P(x)$ is true.
- $\exists_1 ! x P(x)$ is an alternative notation for $\exists ! x P(x)$.
- This is read as
 - There is one and only one x such that $P(x)$.
 - There exists a unique x such that $P(x)$.
- **Example:** Let $P(x)$ denote $x + 1 = 0$ and U are the integers.
 - Then $\exists ! x P(x)$ is true.
- **Example:** Let $P(x)$ denote $x > 0$ and U are the integers.
 - Then $\exists ! x P(x)$ is false.
- The uniqueness quantifier can be expressed by standard operations. $\exists ! x P(x)$ is equivalent to
$$\exists x (P(x) \wedge \forall y (P(y) \rightarrow y = x)).$$

- ◆ Quantifiers \forall and \exists have higher precedence than all logical operators.
- ◆ $\forall x P(x) \wedge Q(x)$ means $(\forall x P(x)) \wedge Q(x)$ In particular, this expression contains a free variable.
- ◆ $\forall x (P(x) \wedge Q(x))$ means something different.

Example

- ◆ Translate the following sentence into predicate logic:
“Every student in this class has taken a course in Java.”
- ◆ Solution:
 - First decide on the domain U (Universe of discourse).
 - Solution 1: If U is all students in this class, define a propositional function $J(x)$ denoting “ x has taken a course in Java” and translate as $\forall x J(x)$.
 - Solution 2: But if U is all people, also define a propositional function $S(x)$ denoting “ x is a student in this class” and translate as $\forall x (S(x) \rightarrow J(x))$
- ◆ Note: $\forall x (S(x) \wedge J(x))$ is not correct. What does it mean?

- ◆ Some student in this class has visited Mexico

- means that
- “There is a student in this class with the property that the student has visited Mexico.”
- We can introduce a variable x , so that our statement becomes
- “There is a student x in this class having the property that x has visited Mexico.”
- $M(x)$, which is the statement “ x has visited Mexico”
- If the domain for x consists
- of the students in this class, we can translate this first statement as $\exists xM(x)$.
- if we are interested in people other than those in this class,
- “There is a person x having the properties that x is a student in this class and x has visited Mexico.”
- $S(x)$ to represent “ x is a student in this class.”
- Solution: $\exists x(S(x) \wedge M(x))$

- ◆ “Every student in this class has visited either Canada or Mexico”
 - $C(x)$ be “ x has visited Canada.”
 - domain for x consists of
 - the students in this class, this second statement can be expressed as $\forall x(C(x) \vee M(x))$.
 - if the domain for x consists of all people
 - “For every person x , if x is a student in this class, then x has visited Mexico or x has visited Canada.”
 - $\forall x(S(x) \rightarrow (C(x) \vee M(x)))$.

Predicates and Quantifiers

Puzzle

Brown, Jones and Smith are suspected of income tax evasion. They testify under oath as follows:

Brown: Jones is guilty and Smith is innocent.

Jones: If Brown is guilty, then so is Smith.

Smith: I am innocent but at least one of the others is guilty.

Assume,

Brown

innocent

guilty

B	I	J	G	G	G	G
J	I	S	I	I	I	I
S	I	J	I	G	I	G
I	J	S	I	I	I	G
X	X	X	✓	X	X	X

$\neg(\neg J \wedge S)$

$J \vee \neg S$

$\left. \begin{array}{l} B \rightarrow \text{guilty} \\ I \rightarrow \text{innocent} \\ S \rightarrow \text{guilty.} \end{array} \right\}$

Real use

- An important type of programming language is designed to reason using the rules of predicate logic. Prolog (from *Programming in Logic*), developed in the 1970s by computer scientists working in the area of artificial intelligence, is an example of such a language. Prolog programs include a set of declarations consisting of two types of statements, **Prolog facts** and **Prolog rules**.
- Prolog facts define predicates by specifying the elements that satisfy these predicates.
- Prolog rules are used to define new predicates using those already defined by Prolog facts.

Quantifiers as Conjunctions/Disjunctions

- If the domain is **finite** then universal/existential quantifiers can be expressed by conjunctions/disjunctions.
- If U consists of the integers 1, 2, and 3, then

$$\begin{aligned}\forall x P(x) &\equiv P(1) \wedge P(2) \wedge P(3) \\ \exists x P(x) &\equiv P(1) \vee P(2) \vee P(3)\end{aligned}$$

- Even if the domains are infinite, you can still think of the quantifiers in this fashion, but the equivalent expressions without quantifiers will be infinitely long.

Negation for Quantifiers

- The rules for negating quantifiers are:
- We can say, De Morgan's Law for Quantifiers

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

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

Negating Quantifiers

- Consider the quantified statement:
 - “Every student has at least one course where the lecturer is a teaching assistant.”
 - Its negation is the statement:
 - “There is a student such that in every course the lecturer is not a teaching assistant.”

Negate each of the following statements

- (a) *All students live in the dormitories.*
- (b) *All mathematics majors are males.*
- (c) *Some students are 25 years old or older.*

solution

- (a) *At least one student does not live in the dormitories.*
(Some students do not live in the dormitories.)
- (b) *At least one mathematics major is female.* (*Some mathematics majors are female.*)
- (c) *None of the students is 25 years old or older.* (*All the students are under 25.*)

Negate each of the following statements:

- (a) $\exists x \forall y, p(x, y);$
- (b) $\exists x \forall y, p(x, y);$
- (c) $\exists y \exists x \forall z, p(x, y, z).$

Use $\neg \forall x p(x) \equiv \exists x \neg p(x)$ and $\neg \exists x p(x) \equiv \forall x \neg p(x);$

Solution

- (a) $\neg(\exists x \forall y, p(x, y)) \equiv \forall x \exists y \neg p(x, y)$
- (b) $\neg(\forall x \forall y, p(x, y)) \equiv \exists x \exists y \neg p(x, y)$
- (c) $\neg(\exists y \exists x \forall z, p(x, y, z)) \equiv \forall y \forall x \exists z \neg p(x, y, z)$

◆ Express the statement “Every student in this class has studied calculus” using predicates and quantifiers.

- rewrite the statement
- “For every student in this class, that student has studied calculus.”
- “For every student x in this class, x has studied calculus.”
 $C(x)$: “ x has studied calculus.”
- domain for x consists of the students in the class
- we can translate our statement as $\forall x C(x)$
- If we change the domain to consist of all people
- “For every person x , if person x is a student in this class then x has studied calculus.”
 $S(x)$: person x is in this class
 $\forall x(S(x) \rightarrow C(x))$.
- Our statement cannot be expressed as $\forall x(S(x) \wedge C(x))$ because this statement says that all people are students in this class and have studied calculus!
- As this property, $P \rightarrow Q \equiv \sim P \vee Q$

- Express the statements “Some student in this class has visited Mexico” and “Every student in this class has visited either Canada or Mexico” using predicates and quantifiers
 - “There is a student in this class with the property that the student has visited Mexico.”
 - “There is a student x in this class having the property that x has visited Mexico.”
 - $M(x)$: x has visited Mexico
- domain for x consists of the students in this class, then $\exists x M(x)$.
 - Domain: all people.
 - “There is a person x having the properties that x is a student in this class and x has visited Mexico.”
 - $S(x)$: “ x is a student in this class.”
 - Now, $\exists x(S(x) \wedge M(x))$

Means: there is a person x who is a student in this class and who has visited Mexico.

- Our statement cannot be expressed as $\exists x(S(x) \rightarrow M(x))$, which is true when there is someone not in the class because, in that case, for such a person x , $S(x) \rightarrow M(x)$ becomes either $F \rightarrow T$ or $F \rightarrow F$, both of which are true.
- Statement becomes,
- “For every x in this class, x has the property that x has visited Mexico or x has visited Canada.”

Example to transfer from English to Logical

- Consider these statements. The first two are premises and the third is the conclusion.
 - “All lions are fierce.”
 - “Some lions do not drink coffee.”
 - “Some fierce creatures do not drink coffee.”
- Solution
 - Let $P(x)$, $Q(x)$ and $R(x)$ be the statements “ x is a lion”, “ x is fierce” and “ x drinks coffee.” respectively. Let the domain consists of all creatures. Now the statements are:
 - $\forall x (P(x) \rightarrow Q(x))$.
 - $\exists x (P(x) \wedge \neg R(x))$.
 - $\exists x (Q(x) \wedge \neg R(x))$.
- Not okay:
 - $\exists x (P(x) \rightarrow \neg R(x))$ here ,if creature is not lion then also they drink coffee.
 - $\exists x (Q(x) \rightarrow \neg R(x))$
- Not exact -- both are true even if $P(x)$ and $Q(x)$ both are not true!

- Consider these statements. The first three are premises and the fourth is a valid conclusion.
 - “All hummingbirds are richly colored.”
 - “No large birds live on honey.”
 - “Birds that do not live on honey are dull in color.”
 - “Hummingbirds are small.”
- Solution
 - Let $P(x)$: “ x is a hummingbird” ,
 - $Q(x)$: “ x is large”,
 - $R(x)$: “ x lives on honey”,
 - $S(x)$: “ x is richly colored.”
 - Let the domain consists of all birds. So the statements are:
 - $\forall x (P(x) \rightarrow S(x))$.
 - $\neg \exists x (Q(x) \wedge R(x))$.
 - $\forall x (\neg R(x) \rightarrow \neg S(x))$.
 - $\forall x (P(x) \rightarrow \neg Q(x))$.

Propositions for More than one variable

Let $B = \{1, 2, 3, \dots, 9\}$ and let $p(x, y)$ denote “ $x + y = 10$ ”
Then $p(x, y)$ is a propositional function.

- The following is a statement since there is a quantifier for each variable:
 - $\forall x \exists y, p(x, y)$, that is, “*For every x, there exists a y such that $x + y = 10$* ”
 - This statement is **true**. For example, if $x = 1$, let $y = 9$; if $x = 2$, let $y = 8$, and so on.
- The following is also a statement:
 - $\exists y \forall x, p(x, y)$, that is, “*There exists a y such that, for every x, we have $x + y = 10$* ”
 - No such y exists; hence this statement is **false**.
- **Note:** Change of order for different quantifiers can change the meaning.

Quantifications of Two Variables

Statement

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

Examples

- Determine the truth value of each of the following statements where $U = \{1, 2, 3\}$ is the universal set:

- (a) $\exists x \forall y, x^2 < y + 1;$
- (b) $\forall x \exists y, x^2 + y^2 < 12;$

Solution

- (a) True. For if $x = 1$, then 1, 2, and 3 are all solutions to $1 < y + 1$.
- (b) True. For each x_0 , let $y = 1$; it is a true statement.

If we change order meaning can get changed.

- Examples:
- $\forall x \exists y$ [x is married to y] is true,
however, $\exists y \forall x$ [x married to y] asserts that there is some person in the universe who married to everyone, this is false .
- $\forall x \exists y$ [$x+y=0$] (for all x, there exists a y such that $x+y=0$ is true, since for any value of s there is a value of y (i.e, $-x$) which makes it true.

However,

- $\exists y \forall x$ [$x+y=0$] (There exists a y such that for all x, $x+y=0$) asserts that value of y can be chosen independently of the value of x, since no y exists which yields zero when added to arbitrary integer x , this is false.

Examples in Mathematics Nested Quantifiers

- Translate the logical statement into Logical.
 1. The sum of two integers is always positive.
 - To solve this, Read “For every two integers, if these integers are both positive, then the sum of these integers is positive”.

$$\forall x \forall y ((x > 0) \wedge (y > 0) \rightarrow (x + y > 0))$$

$$\forall x \forall y (x + y > 0)$$

2. “Every real number expect zero has a multiplicative inverse” (A multiplicative index of a real number x is a real number y such that $xy=1$.)

Solution:

We can rewrite as, “For every real number x expect 0, x has a multiplicative inverse.”

“For every real number x , if $x \neq 0$ ”, then there exists a real number y such that $xy=1$ ”

$$\forall x((x \neq 0) \rightarrow \exists y(xy = 1))$$

Valid, Satisfiable and unsatisfiable

- If $P(x_1, x_2, \dots, x_n)$ is true for all values C_1, C_2, \dots, C_n from the universe U , then $P(x_1, x_2, \dots, x_n)$ is **valid** in U .
- If $P(x_1, x_2, \dots, x_n)$ is true for some values of C_1, C_2, \dots, C_n from the universe U , then $P(x_1, x_2, \dots, x_n)$ is **Satisfiable** in U .
- If $P(x_1, x_2, \dots, x_n)$ is not true for any values of C_1, C_2, \dots, C_n from the universe U , then $P(x_1, x_2, \dots, x_n)$ is **Unsatisfiable** in U .

Nested Quantifiers

- ◆ Complex meanings require nested quantifiers.
 - ◆ “Every real number has an inverse w.r.t. addition.”
 - ◆ Let the domain U be the real numbers. Then the property is expressed by
$$\forall x \exists y (x + y = 0)$$
 - ◆ “Every real number except zero has a multiplicative inverse.”
 - ◆ Let the domain U be the real numbers. Then the property is expressed by
$$\forall x (x \neq 0 \rightarrow \exists y (x * y = 1))$$

Examples on Negation

- ◆ Negate the following :
- ◆ “There does not exist a woman who has taken a flight on every airline in the world ”

Solution:

- ◆ “There is a woman who has taken a flight on every airline in the world ” we can express,

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

Where, $P(w, f)$ is “ w has taken f ” $Q(f, a)$ is “ f is a flight on a ”.

By applying Demorgan’s law for quantifiers we can move negation inside successive quantifiers and by applying this in last step we will get the equation equivalent this.

$$\begin{aligned} & \forall w \neg \forall a \exists f (P(w, f) \wedge Q(f, a)) \\ & \forall w \exists a \neg \exists f (P(w, f) \wedge Q(f, a)) \\ & \forall w \exists a \forall f \neg (P(w, f) \wedge Q(f, a)) \\ & \forall w \exists a \forall f (\neg P(w, f) \vee \neg Q(f, a)) \end{aligned}$$

Set Theory

A set is an unordered collection of objects

English alphabet vowels: $V = \{a, e, i, o, u\}$

$$a \in V \quad b \notin V$$

Odd positive integers less than 10:

$$O = \{1, 3, 5, 7, 9\}$$

elements of set
members of set

Other set representations

Set of positive integers less than 100:

$$\{1, 2, 3, \dots, 99\}$$

omitted
elements

Odd positive integers less than 10:

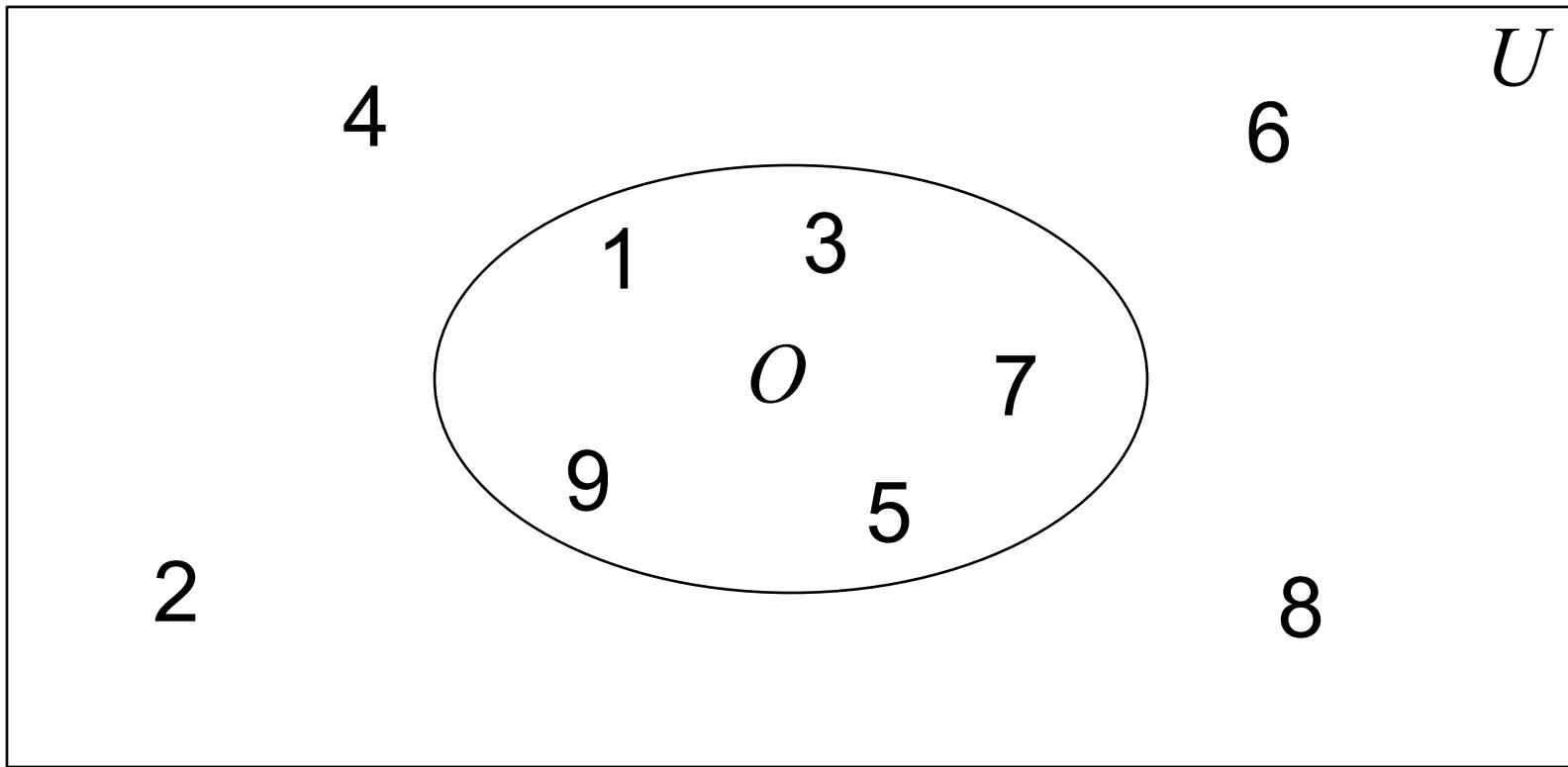
$$O = \{1, 3, 5, 7, 9\}$$

$$O = \{x \mid x \text{ is an odd positive integer less than } 10\}$$

$$O = \{x \in Z^+ \mid x \text{ is odd and } x < 10\}$$

Venn Diagram

Universe



$$U = \{x \mid x \text{ is a positive integer less than } 10\}$$

$$O = \{x \mid x \text{ is an odd positive integer less than } 10\}$$

Useful sets

$$N = \{0, 1, 2, 3, \dots\}$$

Natural numbers

$$Z = \{\dots, -2, 1, 0, 1, 2, \dots\}$$

Integers

$$Z^+ = \{1, 2, 3, \dots\}$$

Positive integers

$$Q = \{p / q \mid p \in Z, q \in Z, q \neq 0\}$$

Rational numbers

$$R = \{\text{set of Real numbers}\}$$

Real numbers

Empty set

$$\emptyset = \{\}$$

$$\emptyset \neq \{\emptyset\}$$

Cardinality (size) of set

Finite sets

$$S_1 = \{a, e, i, o, u\}$$

Number of elements

$$|S_1| = 5$$

$$S_2 = \{a, b, c, \dots, z\}$$

$$|S_2| = 26$$

$$S_3 = \{1, 2, 3, \dots, 99\}$$

$$|S_3| = 99$$

$$|\emptyset| = |\{\}| = 0$$

$$|\{\emptyset\}| = 1$$

Infinite set

$$N = \{0, 1, 2, 3, \dots\}$$

infinite size

Equal sets

$$A = B$$

$$\forall x(x \in A \leftrightarrow x \in B)$$

Examples: $\{1,3,5\} = \{3,5,1\}$

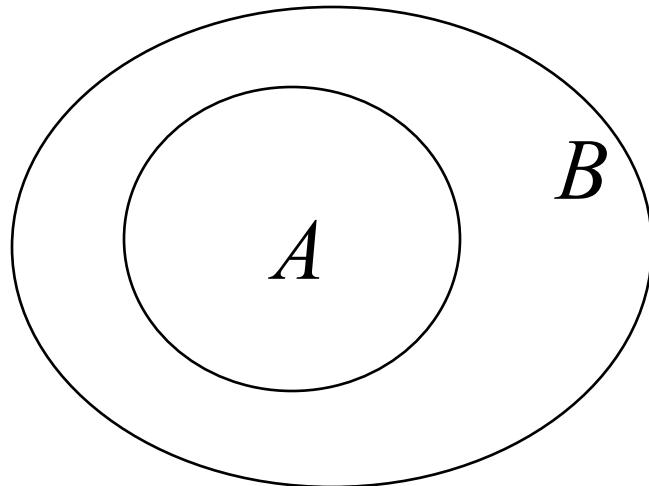
$$\{1,3,5\} = \{1,3,3,3,5,5,5,5\}$$

$$\{1,3,5,7,9\} = \{x \in \mathbb{Z}^+ \mid x \text{ is odd and } x < 10\}$$

Subset

$$A \subseteq B$$

$$\forall x(x \in A \rightarrow x \in B)$$



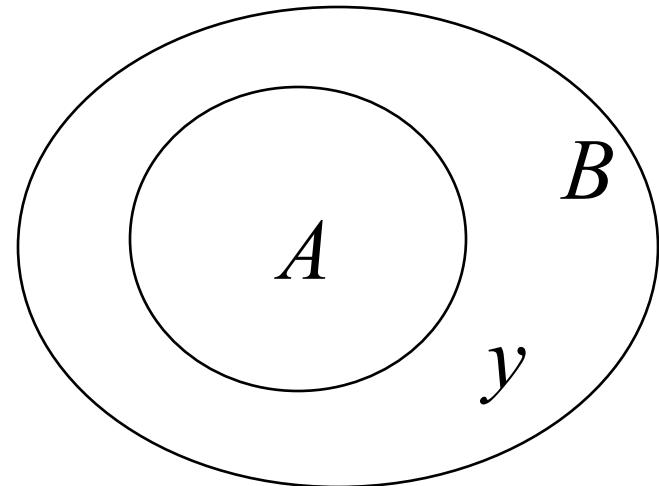
Examples: $\{1,3,5\} \subseteq \{0,1,3,5\}$ $N \subseteq Z$

For any set S $S \subseteq S$ $\emptyset \subseteq S$

Proper Subset

$$A \subset B$$

$$A \subseteq B \wedge A \neq B$$



$$\forall x(x \in A \rightarrow x \in B \wedge \exists y(y \in B \wedge y \notin A))$$

Examples: $\{1,3,5\} \subset \{0,1,3,5\}$ $N \subset Z$

$$A = B$$

is equivalent to

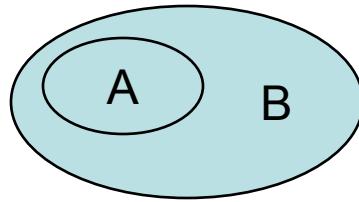
$$A \subseteq B \quad \wedge \quad B \subseteq A$$

Notation

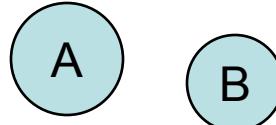
- $S=\{a, b, c\}$ refers to the set whose elements are a, b and c .
- $a \in S$ means “ a is an element of set S ”.
- $d \notin S$ means “ d is *not* an element of set S ”.
- $\{x \in S \mid P(x)\}$ is the set of all those x from S such that $P(x)$ is true. *E.g.*, $T=\{x \in \mathbb{Z} \mid 0 < x < 10\}$.
- **Notes:**
 - 1) $\{a,b,c\}, \{b,a,c\}, \{c,b,a,b,b,c\}$ all represent the same set.
 - 2) Sets can themselves be elements of other sets, *e.g.*, $S=\{\{\text{Mary}, \text{John}\}, \{\text{Tim}, \text{Ann}\}, \dots\}$

Relations between sets

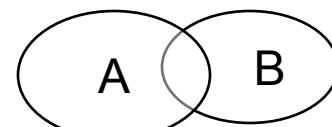
- **Definition:** Suppose A and B are sets. Then
A is called a **subset** of B: $A \subseteq B$
iff every element of A is also an element of B.
Symbolically,
 $A \subseteq B \Leftrightarrow \forall x, \text{ if } x \in A \text{ then } x \in B.$
- $A \not\subseteq B \Leftrightarrow \exists x \text{ such that } x \in A \text{ and } x \notin B.$



$$A \subseteq B$$



$$A \not\subseteq B$$



$$A \not\subseteq B$$

Relations between sets

- **Definition:** Suppose A and B are sets. Then
A **equals** B: $A = B$
iff every element of A is in B and
every element of B is in A.
Symbolically,
 $A=B \Leftrightarrow A \subseteq B \text{ and } B \subseteq A$.
- **Example:** Let $A = \{m \in \mathbb{Z} \mid m=2k+3 \text{ for some integer } k\}$;
 $B = \text{ the set of all odd integers.}$
Then $A=B$.

Operations on Sets

Definition: Let A and B be subsets of a set U .

1. Union of A and B : $A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$

2. Intersection of A and B :

$$A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}$$

3. Difference of B minus A : $B - A = \{x \in U \mid x \in B \text{ and } x \notin A\}$

4. Complement of A : $A^c = \{x \in U \mid x \notin A\}$

Ex.: Let $U = \mathbb{R}$, $A = \{x \in \mathbb{R} \mid 3 < x < 5\}$, $B = \{x \in \mathbb{R} \mid 4 < x < 9\}$.

Then

$$1) A \cup B = \{x \in \mathbb{R} \mid 3 < x < 9\}.$$

$$2) A \cap B = \{x \in \mathbb{R} \mid 4 < x < 5\}.$$

$$3) B - A = \{x \in \mathbb{R} \mid 5 \leq x < 9\}, \quad A - B = \{x \in \mathbb{R} \mid 3 < x \leq 4\}.$$

$$4) A^c = \{x \in \mathbb{R} \mid x \leq 3 \text{ or } x \geq 5\}, \quad B^c = \{x \in \mathbb{R} \mid x \leq 4 \text{ or } x \geq 9\}$$

Properties of Sets

➤ **Theorem 1 (Some subset relations):**

- 1) $A \cap B \subseteq A$
- 2) $A \subseteq A \cup B$
- 3) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

➤ To prove that $A \subseteq B$ use the “**element argument**”:

1. suppose that x is a particular but arbitrarily chosen element of A ,
2. show that x is an element of B .

Proving a Set Property

- **Theorem 2 (Distributive Law):**

For any sets A,B and C:

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

- **Proof:** We need to show that

$$(I) A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C) \text{ and}$$

$$(II) (A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C).$$

Let's show (I).

Suppose $x \in A \cup (B \cap C)$ (1)

We want to show that $x \in (A \cup B) \cap (A \cup C)$ (2)

Proving a Set Property

- **Proof (cont.):**

$$x \in A \cup (B \cap C) \Rightarrow x \in A \text{ or } x \in B \cap C.$$

(a) Let $x \in A$. Then

$$x \in A \cup B \text{ and } x \in A \cup C \Rightarrow x \in (A \cup B) \cap (A \cup C)$$

(b) Let $x \in B \cap C$. Then $x \in B$ and $x \in C$.

$$\left. \begin{array}{l} x \in B \Rightarrow x \in A \cup B \\ x \in C \Rightarrow x \in A \cup C \end{array} \right\} \Rightarrow x \in (A \cup B) \cap (A \cup C)$$

Thus, (2) is true, and we have shown (I).

(II) is shown similarly (*left as exercise*). ■

Set Properties

- Commutative Laws:

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

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

- Associative Laws:

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

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

- Distributive Laws:

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

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

Set Properties

- Double Complement Law:

$$(A^c)^c = A$$

- De Morgan's Laws:

$$(a) (A \cap B)^c = A^c \cup B^c$$

$$(b) (A \cup B)^c = A^c \cap B^c$$

- Absorption Laws:

$$(a) A \cup (A \cap B) = A$$

$$(b) A \cap (A \cup B) = A$$

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

Proof: Show that $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$ and $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$

Part 1: $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$

$$x \in \overline{A \cap B}$$

$$\rightarrow x \notin A \cap B \rightarrow \neg(x \in A \cap B) \quad \text{De Morgan's law from logic}$$

$$\rightarrow \neg((x \in A) \wedge (x \in B)) \rightarrow \neg(x \in A) \vee \neg(x \in B)$$

$$\rightarrow (x \notin A) \vee (x \notin B) \rightarrow (x \in \overline{A}) \vee (x \in \overline{B})$$

$$\rightarrow x \in (\overline{A} \cup \overline{B})$$

Part 2: $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$

$$x \in (\overline{A} \cup \overline{B})$$

$$\rightarrow (x \in \overline{A}) \vee (x \in \overline{B}) \rightarrow (x \notin A) \vee (x \notin B)$$

$$\rightarrow \neg(x \in A) \vee \neg(x \in B) \rightarrow \neg((x \in A) \wedge (x \in B))$$

$$\rightarrow \neg(x \in A \cap B) \quad \text{De Morgan's law from logic}$$

$$\rightarrow x \in \overline{A \cap B}$$

End of Proof

Showing that a set property is false

- **Statement:** For all sets A,B and C,

$$A - (B - C) = (A - B) - C .$$

The following **counterexample** shows that the statement is **false**.

- **Counterexample:**

Let $A = \{1, 2, 3, 4\}$, $B = \{3, 4, 5, 6\}$, $C = \{3\}$.

Then $B - C = \{4, 5, 6\}$ and $A - (B - C) = \{1, 2, 3\}$.

On the other hand,

$A - B = \{1, 2\}$ and $(A - B) - C = \{1, 2\}$.

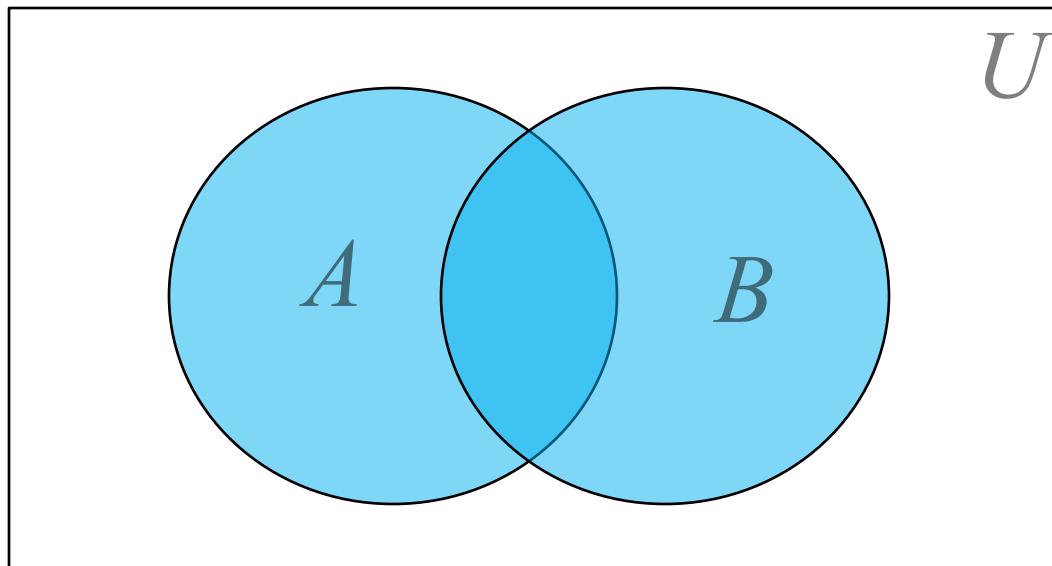
Thus, for this example

$$A - (B - C) \neq (A - B) - C .$$

Set operations

Union

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$



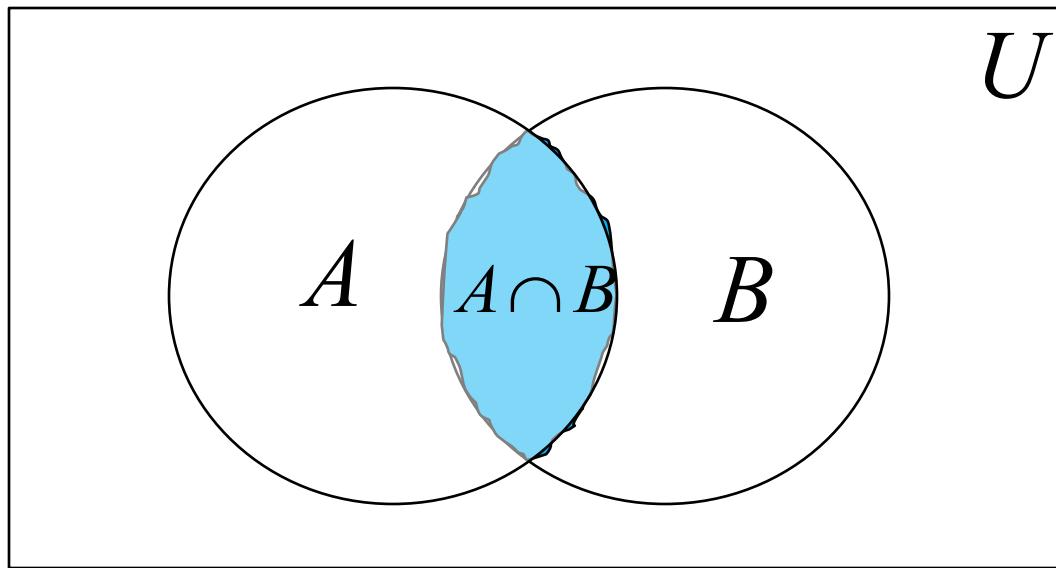
$$A = \{1, 3, 5\}$$

$$B = \{1, 2, 3\}$$

$$A \cup B = \{1, 2, 3, 5\}$$

Intersection

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$



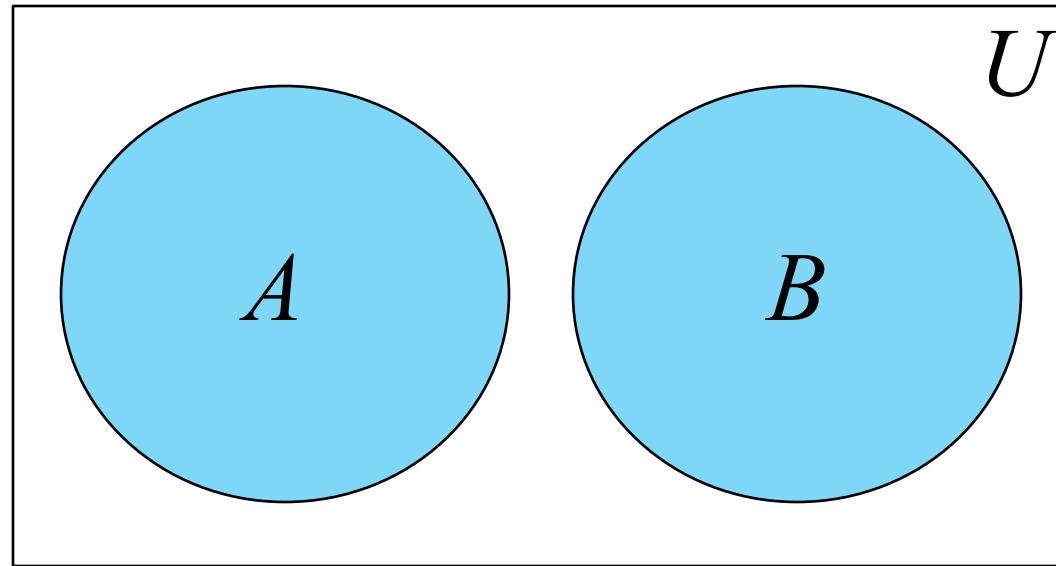
$$A = \{1, 3, 5\}$$

$$B = \{1, 2, 3\}$$

$$A \cap B = \{1, 3\}$$

Disjoint sets A, B

$$A \cap B = \emptyset$$



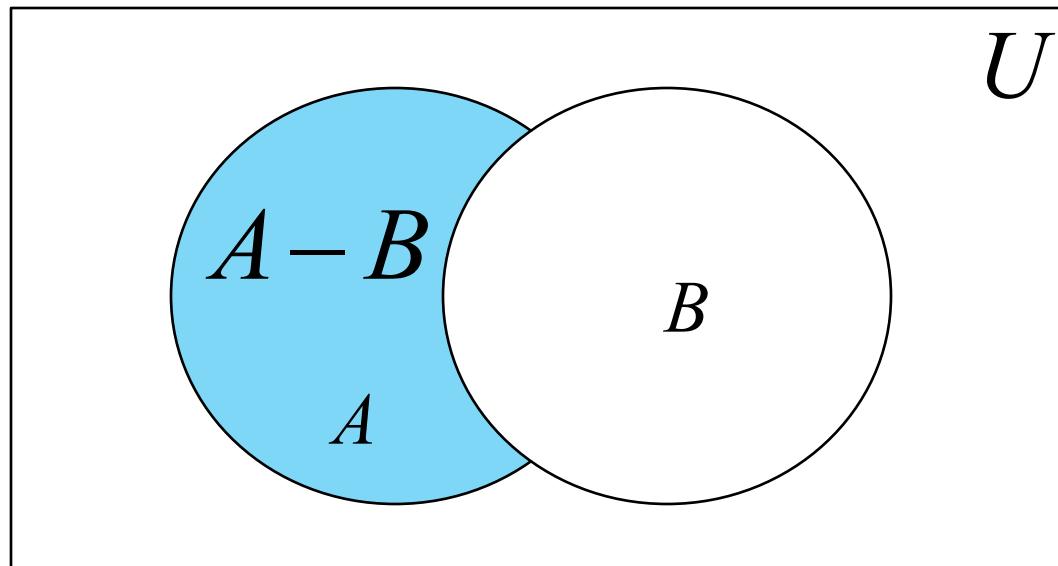
$$A = \{1, 3, 5\}$$

$$B = \{2, 9\}$$

$$A \cap B = \emptyset$$

Set difference

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$



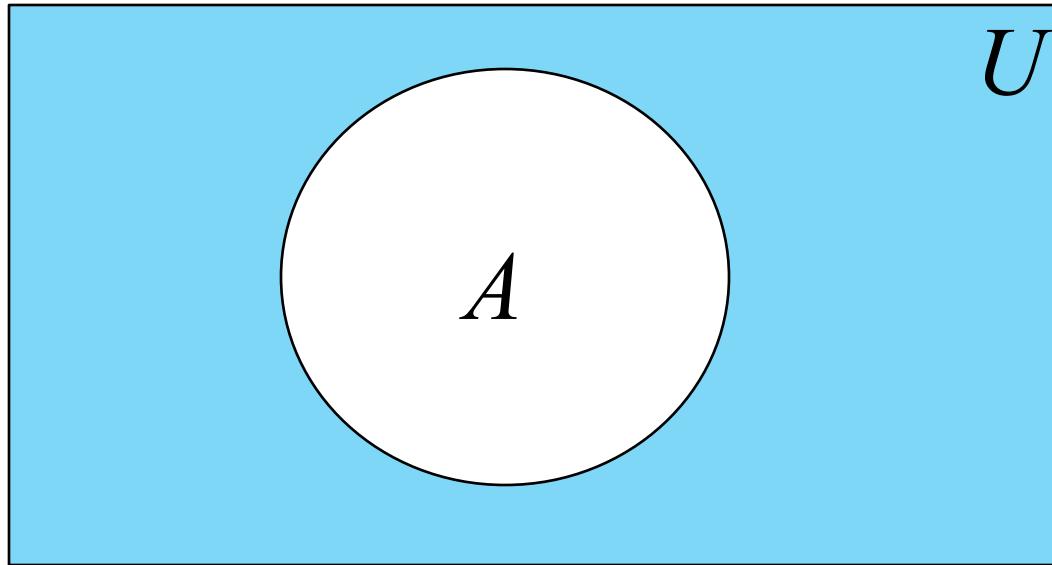
$$A = \{1, 3, 5\}$$

$$B = \{1, 2, 3\}$$

$$A - B = \{5\}$$

Complement

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



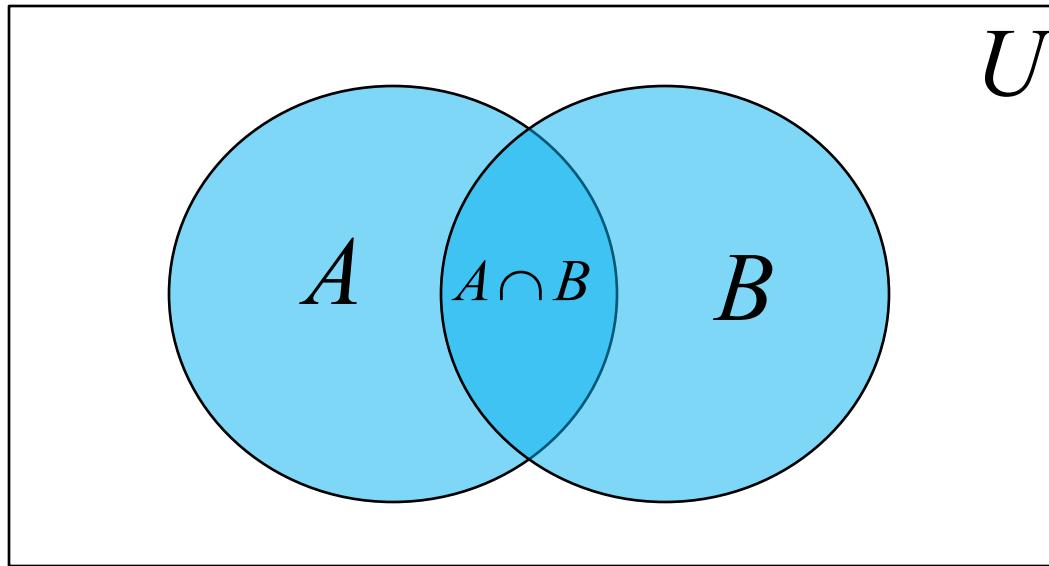
$$A = \{1, 3, 5\}$$

$$U = \{1, 2, 3, 4, 5\}$$

$$\overline{A} = \{2, 4\}$$

Size of union

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



$$A = \{1, 3, 5\} \quad B = \{1, 2, 3\} \quad A \cup B = \{1, 2, 3, 5\} \quad A \cap B = \{1, 3\}$$

$$|A \cup B| = |A| + |B| - |A \cap B| = 3 + 3 - 2 = 4$$

Empty Set

- The unique set with no elements
is called **empty set** and denoted by \emptyset .
- Set Properties that involve \emptyset .
For all sets A,
 1. $\emptyset \subseteq A$
 2. $A \cup \emptyset = A$
 3. $A \cap \emptyset = \emptyset$
 4. $A \cap A^c = \emptyset$

Disjoint Sets

- A and B are called **disjoint** iff $A \cap B = \emptyset$.
- Sets A_1, A_2, \dots, A_n are called **mutually disjoint** iff for all $i, j = 1, 2, \dots, n$
$$A_i \cap A_j = \emptyset \text{ whenever } i \neq j.$$
- Examples:
 - 1) $A=\{1,2\}$ and $B=\{3,4\}$ are disjoint.
 - 2) The sets of even and odd integers are disjoint.
 - 3) $A=\{1,4\}$, $B=\{2,5\}$, $C=\{3\}$ are mutually disjoint.
 - 4) $A-B$, $B-A$ and $A \cap B$ are mutually disjoint.

Partitions

- **Definition:** A collection of nonempty sets $\{A_1, A_2, \dots, A_n\}$ is a **partition** of a set A iff
 1. $A = A_1 \cup A_2 \cup \dots \cup A_n$
 2. A_1, A_2, \dots, A_n are mutually disjoint.
- *Examples:*
 - 1) $\{\mathbb{Z}^+, \mathbb{Z}^-, \{0\}\}$ is a partition of \mathbb{Z} .
 - 2) Let $S_0 = \{n \in \mathbb{Z} \mid n=3k \text{ for some integer } k\}$
 $S_1 = \{n \in \mathbb{Z} \mid n=3k+1 \text{ for some integer } k\}$
 $S_2 = \{n \in \mathbb{Z} \mid n=3k+2 \text{ for some integer } k\}$
Then $\{S_0, S_1, S_2\}$ is a partition of \mathbb{Z} .

Power Sets

- **Definition:** Given a set A,
the **power set** of A, denoted $\mathcal{P}(A)$,
is the set of all subsets of A.
- *Example:* $\mathcal{P}(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$.
- **Properties:**
 - 1) If $A \subseteq B$ then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
 - 2) If a set A has n elements
then $\mathcal{P}(A)$ has 2^n elements.

Power set

The power set of S contains all possible subsets of S (and the empty set)

$$S = \{1,2,3\}$$

Power set

$$P(S) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$$

$$|P(S)| = 2^{|S|} = 2^3 = 8$$

A curly brace is positioned below the equation $|P(S)| = 2^{|S|} = 2^3 = 8$, spanning its width.

Size of
power set

Special cases

$$P(\emptyset) = \{\emptyset\}$$

$$P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$$

Cartesian product

Cartesian product of two sets A, B

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$$

Example: $A = \{1, 2\}$ $B = \{a, b, c\}$

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$$

$$B \times A = \{(a, 1), (b, 1), (c, 1), (a, 2), (b, 2), (c, 2)\}$$

For this case: $A \times B \neq B \times A$

Size: $|A \times B| = |A| \times |B| = 2 \times 3 = 6$

Cartesian product of sets A_1, A_2, \dots, A_n

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i\}$$

Example: $A = \{1, 2\}$ $B = \{a, b, c\}$ $C = \{x, y\}$

$$A \times B \times C = \{(1, a, x), (1, b, x), (1, c, x), (2, a, x), (2, b, x), (2, c, x), (1, a, y), (1, b, y), (1, c, y), (2, a, y), (2, b, y), (2, c, y)\}$$

Size: $|A \times B \times C| = |A| \times |B| \times |C| = 2 \times 3 \times 2 = 12$

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \times |A_2| \times \cdots \times |A_n|$$

Theorem (Inclusion–Exclusion Principle)

- Suppose A and B are finite sets. Then $A \cup B$ and $A \cap B$ are finite and
$$n(A \cup B) = n(A) + n(B) - n(A \cap B) \text{ or}$$
$$|A \cup B| = |A| + |B| - |A \cap B|$$
- That is, we find the number of elements in A or B (or both) by first adding $n(A)$ and $n(B)$ (inclusion) and then
- subtracting $n(A \cap B)$ (exclusion) since its elements were counted twice.
- Let A,B,C be the finite sets . Then
$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$$

Example For Inclusion Exclusion Formula

- A computer company wants to hire 25 programmers to handle systems programming jobs and 40 programmers for applications programming. Of those hired , ten will be expected to perform jobs of both types. How many programmers must be hired.
- **Solutions:**
 - Let A be the set of systems programmers hired and B be the set of applications programmers hired.
 - The company must have $|A|=25$, $|B|=40$, and $|A \cap B|=10$.
 - The number of programmers that must be hired is $|A \cup B|$, but
$$|A \cup B| = |A| + |B| - |A \cap B|\\ = 25 + 40 - 10\\ = 55$$

Example 2

- Verify $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$
where A={1,2,3,4,5}, B={2,3,4,6}, C={3,4,6,8}.

Solution:

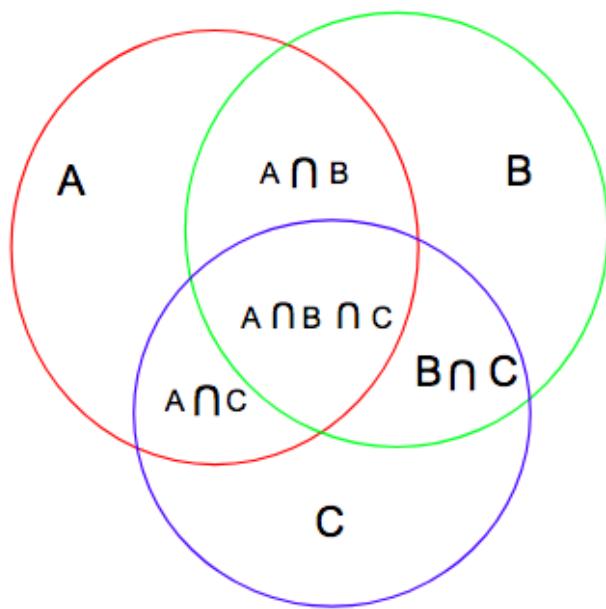
$$A \cup B \cup C = \{1, 2, 3, 4, 5, 6, 8\}$$

$$A \cap B = \{2, 3, 4\}, B \cap C = \{3, 4, 6\} \text{ and } C \cap A = \{3, 4\}$$

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

$$= 5 + 4 + 4 - 3 - 3 - 2 + 2$$

$$= 7 = |A \cap B \cap C|$$



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

Find the number of mathematics students at a college taking at least one of the languages French, German, and Russian given the following data:

65 study French	20 study French and German
45 study German	25 study French and Russian
42 study Russian	15 study German and Russian
8 study all three languages	

We want to find $n(F \cup G \cup R)$ where, F , G , and R denote the sets of students studying French, German, and Russian, respectively.

By the inclusion-exclusion principle,

$$\begin{aligned}n(F \cup G \cup R) &= n(F) + n(G) + n(R) - n(F \cap G) - n(F \cap R) - n(G \cap R) \\&\quad + n(F \cap G \cap R) \\&= 65 + 45 + 42 - 20 - 25 - 15 + 8 = 100\end{aligned}$$

Thus 100 students study at least one of the languages.

Now, suppose we have any finite number of finite sets, say, A_1, A_2, \dots, A_m . Let s_k be the sum of the cardinalities

$$n(A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k})$$

of all possible k -tuple intersections of the given m sets. Then we have the following general inclusion-exclusion principle.

How many binary strings of length 8 either start with a '1' bit or end with two bits '00'?

- **Solution:** If the string starts with one, there are 7 characters left which can be filled in $2^7=128$ ways.
If the string ends with '00' then 6 characters can be filled in $2^6=64$ ways.
Now if we add the above sets of ways and conclude that it is the final answer, then it would be wrong.
- This is because there are strings with start with '1' and end with '00' both, and since they satisfy both criteria they are counted twice.
So we need to subtract such strings to get a correct count.
Strings that start with '1' and end with '00' have five characters that can be filled in $2^5=32$ ways.
- So by the inclusion-exclusion principle we get-
Total strings = $128 + 64 - 32 = 160$

- In case of the usage of three toothpastes A,B,C, It is fount that 60 people like A, 55 like C, 40 like B, 20 like A and B, 35 like B and C, 15 like A and C , and 10 like all three toothpastes. Find the following
 - Number of persons included in the survey.
 - Number of persons who like A only
 - Number of persons who like A and B but not C

- In case of the usage of three toothpastes A,B,C, It is found that 60 people like A, 55 like C, 40 like A and B, 35 like B and C, 15 like A and C , and 10 like all three toothpastes. Find the following
 - Number of persons included in the survey.
 - Number of persons who like A only
 - Number of persons who like A and B but not C

Solution A,B,C, Denote set of people who like toothpastes A, B and C resp.
 given, $|A|=60$, $|B|=55$, $|C|=40$, $|A \cap B|=20$, $|B \cap C|=35$, $|A \cap C|=15$, and
 $|A \cap B \cap C|=10$

Number of persons included in the survey.

$$\begin{aligned}|A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C| \\&= 60 + 55 + 40 - 20 - 35 - 15 + 10 = 95\end{aligned}$$

Number of persons who like A only

$$= |A| - (|A \cap B| + |A \cap C| - |A \cap B \cap C|) = 60 - (20 + 15 - 10) = 35$$

Number of persons who like A and B but not C

$$= |A \cap B| + |A \cap B \cap C| = 20 - 10 = 10$$

Countable Sets

Countable finite set:

Any finite set is countable by default

Countable infinite set:

An infinite set S is countable if there is a one-to-one correspondence from S to \mathbb{Z}^+

Positive integers

Theorem: Even positive integers
are countable

Proof:

Even positive integers: 2, 4, 6, 8, ...

One-to-one
Correspondence:

Positive integers: 1, 2, 3, 4, ...

n corresponds to $2n$

End of Proof

Theorem: The set of rational numbers is countable

Proof:

We need to find a method to list

all rational numbers: $\frac{1}{2}, \frac{3}{4}, \frac{7}{8}, \dots$

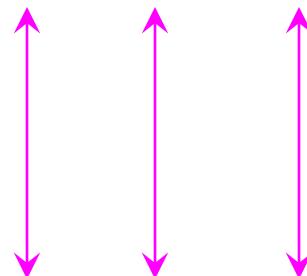
Naïve Approach

Start with nominator=1

Rational numbers:

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

One-to-one
correspondence:



Positive integers:

$$1, 2, 3, \dots$$

Doesn't work:

we will never list
numbers with nominator 2:

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

Better Approach: scan diagonals

Nomin.=1	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$...
Nomin.=2	$\frac{2}{1}$	$\frac{2}{2}$	$\frac{2}{3}$...	
Nomin.=3	$\frac{3}{1}$	$\frac{3}{2}$...		
Nomin.=4	$\frac{4}{1}$...			

first diagonal

$$\frac{1}{1}$$

$$\frac{1}{2}$$

$$\frac{1}{3}$$

$$\frac{1}{4}$$

...

$$\frac{2}{1}$$

$$\frac{2}{2}$$

$$\frac{2}{3}$$

...

$$\frac{3}{1}$$

$$\frac{3}{2}$$

...

$$\frac{4}{1}$$

...

second diagonal

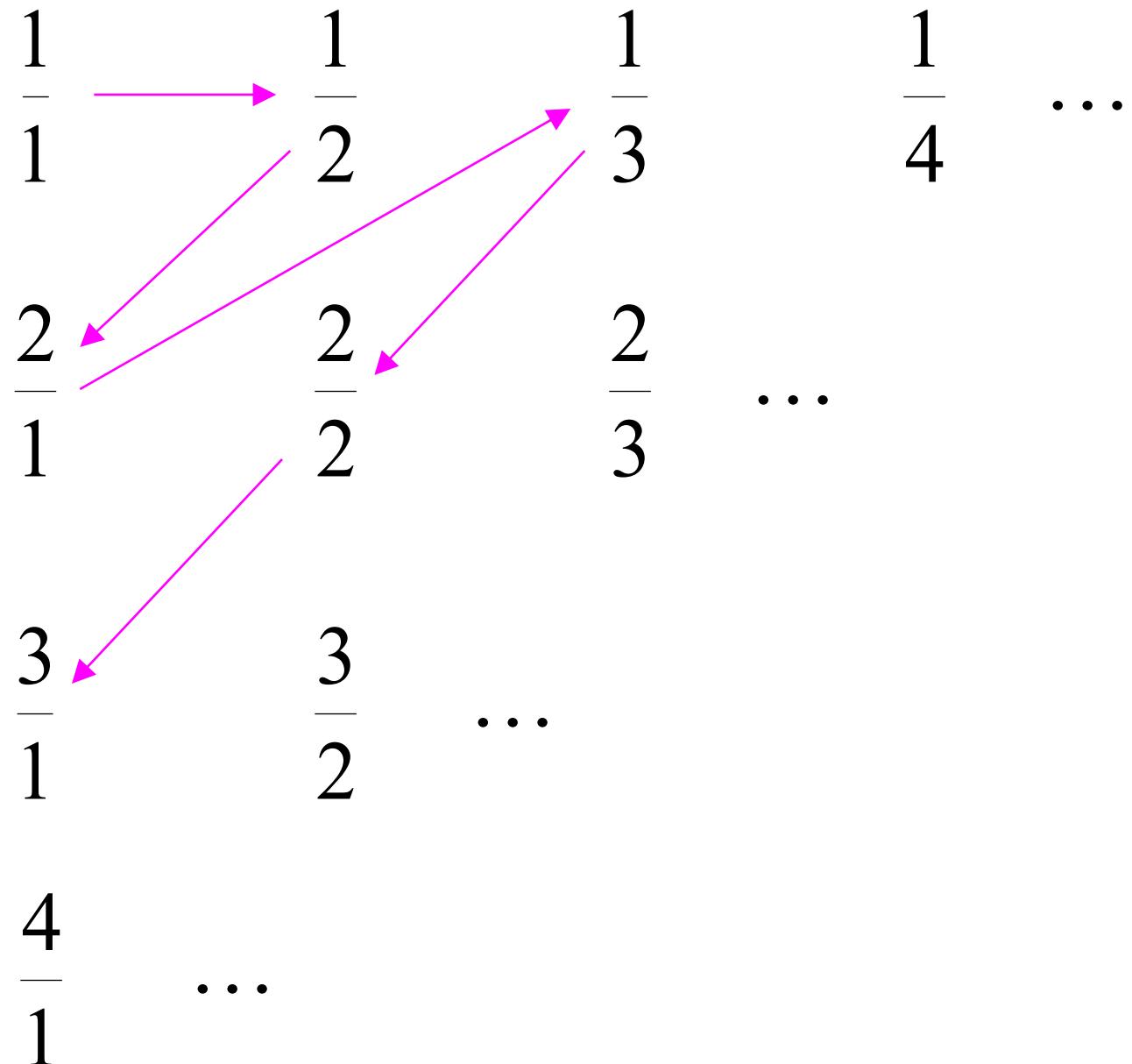
$$\begin{array}{cccc} \frac{1}{1} & \xrightarrow{\hspace{2cm}} & \frac{1}{2} & \quad \frac{1}{3} \\ & \nearrow & & & \frac{1}{4} & \dots \end{array}$$

$$\begin{array}{ccc} \frac{2}{1} & \leftarrow & \frac{2}{2} \\ & & \frac{2}{3} & \dots \end{array}$$

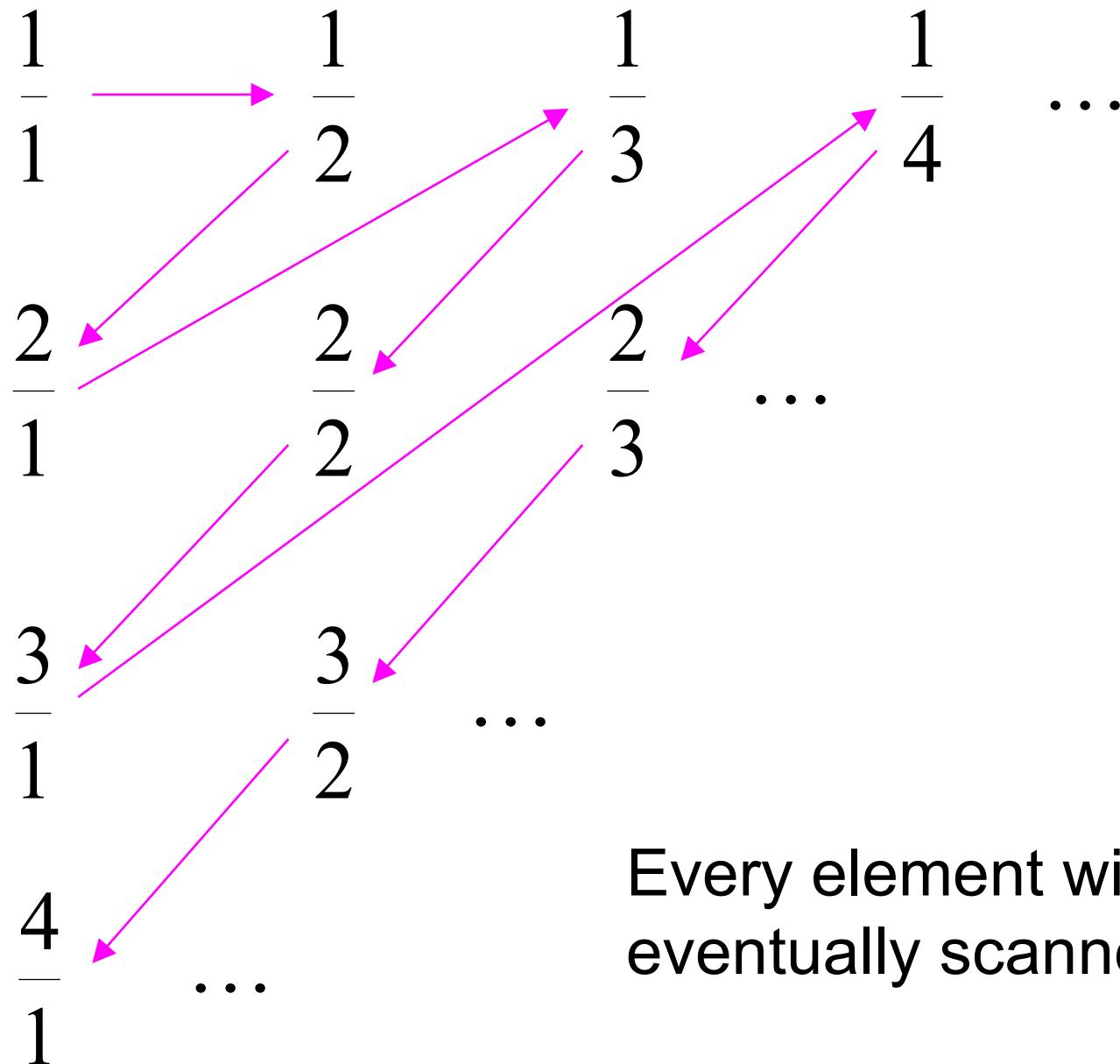
$$\begin{array}{cc} \frac{3}{1} & \frac{3}{2} \\ & \dots \end{array}$$

$$\begin{array}{c} 4 \\ \hline 1 \\ \dots \end{array}$$

third diagonal



fourth diagonal...



Every element will be eventually scanned

Diagonal listing

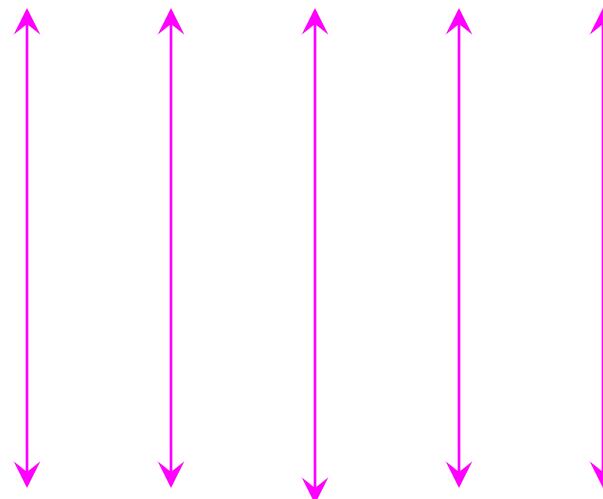
Rational Numbers:

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

One-to-one
correspondence:

Positive Integers:

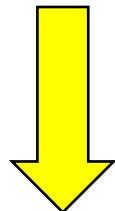
1, 2, 3, 4, 5, ...



End of Proof
54

We have proven: $(0,1) \subseteq R$ is uncountable

It can be proven: Every subset of a countable set is countable



It follows that the set of real numbers R is uncountable

Multisets

- Sets:
 - An unordered collection of distinct objects.
- Multisets:
 - Sets in which some elements occur more than once
 - $A=\{1,1,1,2,2,3\}$
- Notation to represent a multiset by:
 - $S=\{n_1.a_1, n_2.a_2, \dots, n_i.a_i\}$
 - This denotes that a_1 occurs n_1 times
 - The number $n_i=1,2,3,\dots$ Are called multiplicities of the elements n_i .
 - $A=\{3.1,2.2,1.3\}$

Union of Multisets

- The union of the multisets A and B is the multiset where the multiplicity of an element is the maximum of its multiplicities in A and B

$A = \{1, 1, 1, 2, 2, 3\}$ and

$B = \{1, 1, 4, 3, 3\}$

$A \cup B = \{1, 1, 1, 4, 2, 2, 3, 3\}$

Intersection Multisets

- The Intersection of A and B is the multiset where the multiplicity of an element the minimum of its multiplicities in A and B.

$$A = \{1, 1, 1, 2, 2, 3\} \text{ and}$$

$$B = \{1, 1, 4, 3, 3\}$$

$$A \cap B = \{1, 1, 3\}$$

Difference of Multisets

- The difference of A and B is the multiset where the multiplicity of an element is the multiplicity of element in A less its multiplicity in B unless this difference is negative, in which case the multiplicity is zero.

$$A = \{1, 1, 1, 2, 2, 3, 4, 4, 5\}$$

$$B = \{1, 1, 2, 2, 2, 3, 3, 4, 4, 6\}$$

$$A - B = \{1, 5\}$$

Sum of Multisets

- The Sum of A and B is the multiset where the multiplicity of an element is sum of multiplicities in set A and set B denoted by $A+B$.

$$A = \{1, 1, 2, 3, 3\} \quad \text{and} \quad B = \{1, 2, 2, 4\},$$

$$A + B = \{1, 1, 1, 2, 2, 2, 3, 3, 4\}$$

Multiset Examples

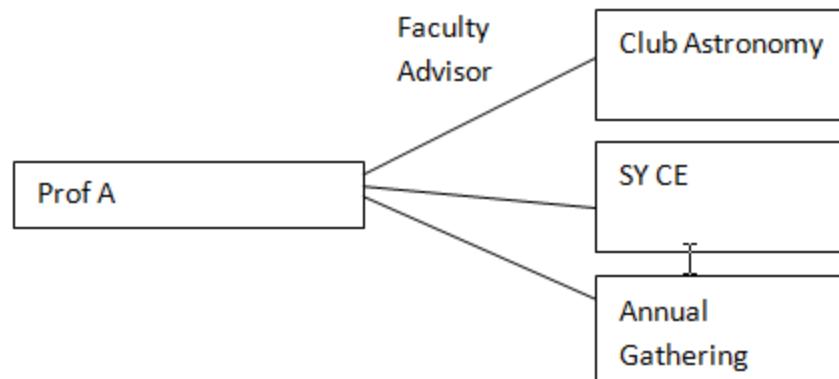
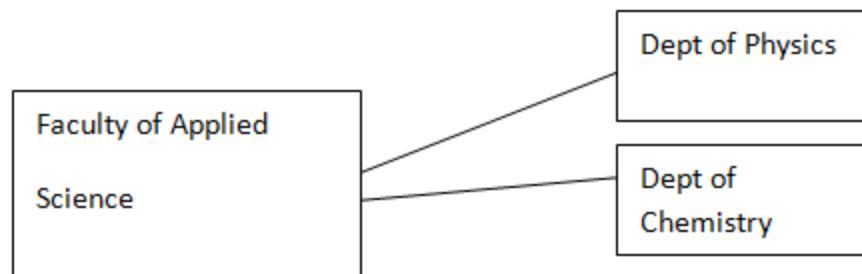
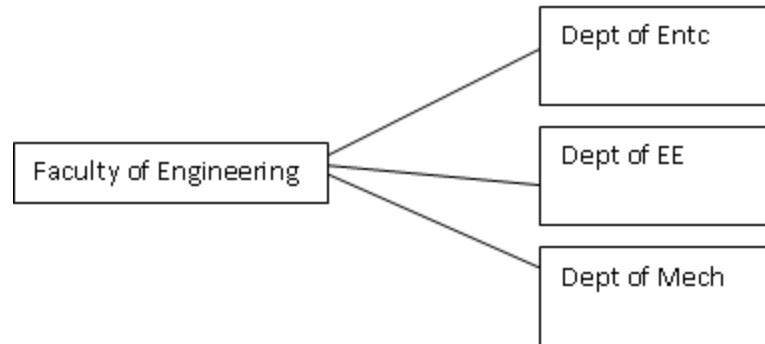
Let A and B be multisets as $A = \{3.a, 2.b, 1.c\}$ and $B = \{2.a, 3.b, 4.d\}$

Find

- (a) $A \cup B = \{3.a, 3.b, 1.c, 4.d\}$
- (b) $A \cap B = \{2.a, 2.b\}$
- (c) $A - B = \{1.a, 1.c\}$
- (d) $B - A = \{1.b, 4.d\}$
- (e) $A + B = \{5.a, 5.b, 1.c, 4.d\}$

Unit 2: Relations, Functions and Recurrence Relations

Relations



Relations

- If we want to describe a relationship between elements of two sets A and B , we can use **ordered pairs** with their first element taken from A and their second element taken from B .
- Since this is a relation between **two sets**, it is called a **binary relation**.
- **Definition:** Let A and B be sets. A binary relation from A to B is a subset of $A \times B$.
- In other words, for a binary relation R we have $R \subseteq A \times B$. We use the notation aRb to denote that $(a, b) \in R$ and \underline{aRb} to denote that $(a, b) \notin R$.

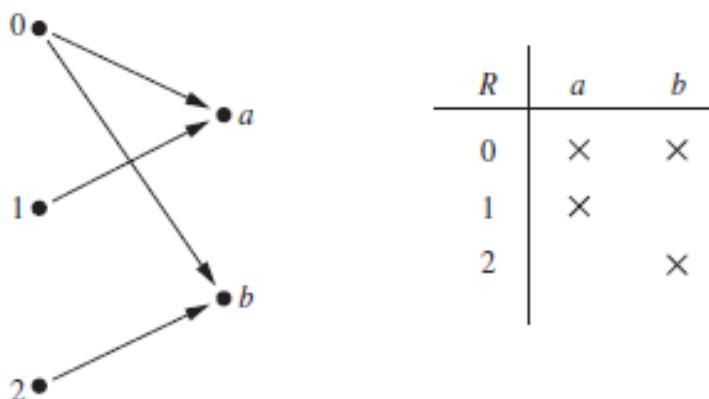
- When (a, b) belongs to R , a is said to be **related** to b by R .
- **Example:** Let P be a set of people, C be a set of cars, and D be the relation describing which person drives which car(s).
 - $P = \{\text{Carl, Suzanne, Peter, Carla}\}$,
 - $C = \{\text{Mercedes, BMW, tricycle}\}$
 - $D = \{(\text{Carl, Mercedes}), (\text{Suzanne, Mercedes}), (\text{Suzanne, BMW}), (\text{Peter, tricycle})\}$
 - This means that Carl drives a Mercedes, Suzanne drives a Mercedes and a BMW, Peter drives a tricycle, and Carla does not drive any of these vehicles.

Relations

sets of ordered pairs are called binary relations.

- Let $A = \{0, 1, 2\}$ and $B = \{a, b\}$. Then $\{(0, a), (0, b), (1, a), (2, b)\}$ is a relation from A to B .

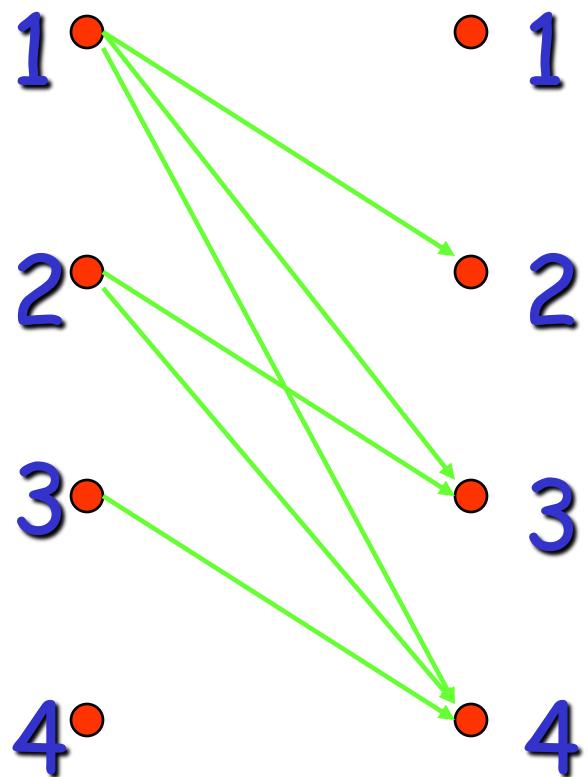
This means, for instance, that $0 R a$, but that $1 R b$.



Relations on set

- **Definition:** A relation on the set A is a relation from A to A .
- In other words, a relation on the set A is a subset of $A \times A$.
- **Example:** Let $A = \{1, 2, 3, 4\}$. Which ordered pairs are in the relation $R = \{(a, b) \mid a < b\}$?

- Solution: $R = \{(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\}$



R	1	2	3	4
1		X	X	X
2			X	X
3				X
4				

Relations and Their Properties

A binary relation from set A to B
is a subset of Cartesian product $A \times B$

Example: $A = \{0,1,2\}$ $B = \{a,b\}$

A relation: $R = \{(0,a), (0,b), (1,a), (2,b)\}$

- How many different relations can we define on a set A with n elements?
 - A relation on a set A is a subset of $A \times A$.
 - How many elements are in $A \times A$?
-
- There are n^2 elements in $A \times A$, so how many subsets (= relations on A) does $A \times A$ have?
 - The number of subsets that we can form out of a set with m elements is 2^m , here $m = n^2$ for $A \times A$. Therefore, 2^{n^2} subsets can be formed out of $A \times A$.
 - **Answer:** We can define 2^{n^2} different relations on A .
 - For example, there are $2^{3^9} = 512$ relations on the set $\{a, b, c\}$.

- Example: Let $A = \{1, 2\}$
- • What is $A \times A = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$
- • List of possible relations (subsets of $A \times A$):
 - \emptyset 1
 - $\{(1,1)\} \{(1,2)\} \{(2,1)\} \{(2,2)\}$ 4
 - $\{(1,1), (1,2)\} \{(1,1),(2,1)\} \{(1,1),(2,2)\}$ 6
 $\{(1,2),(2,1)\} \{(1,2),(2,2)\} \{(2,1),(2,2)\}$
 - $\{(1,1),(1,2),(2,1)\} \{(1,1),(1,2),(2,2)\}$ 4
 $\{(1,1),(2,1),(2,2)\} \{(1,2),(2,1),(2,2)\}$
 - $\{(1,1),(1,2),(2,1),(2,2)\}$ 1
 - Use formula: $2^4 = 16$

Types of Relations

A relation on set A is a subset of $A \times A$

Example:

A relation on set $A = \{1,2,3,4\}$:

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

Reflexive relation R on set A :

$$\forall a \in A, \quad (a, a) \in R$$

Example: $A = \{1, 2, 3, 4\}$

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

Is the “divides” relation on the set of positive integers reflexive?

Solution: Because $a \mid a$ whenever a is a positive integer, the “divides” relation is reflexive.

(Note that if we replace the set of positive integers with the set of all integers the relation is not reflexive because by definition 0 does not divide 0.)

Example

□ Solution: Consider the following relations on $\{1, 2, 3, 4\}$:

$$R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\},$$

$$R_2 = \{(1, 1), (1, 2), (2, 1)\},$$

$$R_3 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\},$$

$$R_4 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\},$$

$$R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\},$$

$R_6 = \{(3, 4)\}$. Which of these relations are reflexive?

The relations R_3 and R_5 are reflexive because they both contain all pairs of the form (a, a) , namely, $(1, 1), (2, 2), (3, 3)$, and $(4, 4)$.

The other relations are not reflexive because

they do not contain all of these ordered pairs. In particular, R_1, R_2, R_4 , and R_6 are not reflexive

because $(3, 3)$ is not in any of these relations.

- Are the following relations on $\{1, 2, 3, 4\}$ reflexive?
- $R = \{(1, 1), (1, 2), (2, 3), (3, 3), (4, 4)\}$ No
- $R = \{(1, 1), (2, 2), (2, 3), (3, 3), (4, 4)\}$ yes
- $R = \{(1, 1), (2, 2), (3, 3)\}$ No

Symmetric relation R :

$$(a,b) \in R \rightarrow (b,a) \in R$$

Example: $A = \{1,2,3,4\}$

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

Asymmetric relation R :

$$(a, b) \in R \rightarrow (b, a) \notin R$$

A relation is said to be asymmetric if it is both antisymmetric and irreflexive or else it is not.

Example: $A = \{1, 2, 3, 4\}$

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

Antisymmetric relation R :

$$(a, b) \in R \wedge (b, a) \in R \rightarrow a = b$$

Example: $A = \{1, 2, 3, 4\}$

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

Properties of Relations

- Are the following relations on $\{1, 2, 3, 4\}$ symmetric, antisymmetric, or asymmetric?

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

$R = \{(1, 1)\}$ **sym. and
antisym.**

$R = \{(1, 3), (3, 2), (2, 1)\}$ **antisym. and
asym.**

$R = \{(4, 4), (3, 3), (1, 4)\}$ **antisym.**

In last example

- ✓ The relations R_2 and R_3 are symmetric, because in each case (b, a) belongs to the relation whenever (a, b) does.
- ✓ For R_2 , the only thing to check is that both $(2, 1)$ and $(1, 2)$ are in the relation.
- ✓ For R_3 , it is necessary to check that both $(1, 2)$ and $(2, 1)$ belong to the relation, and $(1, 4)$ and $(4, 1)$ belong to the relation.
- ✓ This is done by finding a pair (a, b) such that it is in the relation but (b, a) is not.

In last example

- ✓ R_4, R_5 , and R_6 are all antisymmetric. For each of these relations there is no pair of elements a and b with $a = b$ such that both (a, b) and (b, a) belong to the relation.
- ✓ This is done by finding a pair (a, b) with $a = b$ such that (a, b) and (b, a) are both in the relation.

Is the “divides” relation on the set of positive integers symmetric? Is it antisymmetric?

Solution: This relation is not symmetric because $1 \mid 2$, but $2 \nmid 1$. It is antisymmetric, for if a and b are positive integers with $a \mid b$ and $b \mid a$, then $a = b$

Transitive relation R :

$$(a,b) \in R \wedge (b,c) \in R \rightarrow (a,c) \in R$$

Example: $A = \{1,2,3,4\}$

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

In same Example

- R_4, R_5 , and R_6 are transitive. For each of these relations, we can show that it is transitive by verifying that if (a, b) and (b, c) belong to this relation, then (a, c) also does.
- For instance, R_4 is transitive, because $(3, 2)$ and $(2, 1)$, $(4, 2)$ and $(2, 1)$, $(4, 3)$ and $(3, 1)$, and $(4, 3)$ and $(3, 2)$ are the only such sets of pairs, and $(3, 1)$, $(4, 1)$, and $(4, 2)$ belong to R_4 .
- R_1 is not transitive because $(3, 4)$ and $(4, 1)$ belong to R_1 , but $(3, 1)$ does not.
- R_2 is not transitive because $(2, 1)$ and $(1, 2)$ belong to R_2 , but $(2, 2)$ does not.
- R_3 is not transitive because $(4, 1)$ and $(1, 2)$ belong to R_3 , but $(4, 2)$ does not.

Is the “divides” relation on the set of positive integers transitive?

Solution: Suppose that a divides b and b divides c. Then there are positive integers k and l such that $b = ak$ and $c = bl$. Hence, $c = a(kl)$, so a divides c. It follows that this relation is transitive.

How many reflexive relations are there on a set with n elements?

Solution:

A relation R on a set A is a subset of $A \times A$.

Consequently, a relation is determined by specifying whether each of the ordered pairs in $A \times A$ is in R .

However, if R is reflexive, each of the n ordered pairs (a, a) for $a \in A$ must be in R .

Each of the other $n(n - 1)$ ordered pairs of the form (a, b) , where $a \neq b$, may or may not be in R .

Hence, by the product rule for counting, $2^{n(n-1)}$ reflexive relations [this is the number of ways to choose whether each element (a, b) , with $a \neq b$, belongs to R].

Relations of Relations summary

	=	<	>	\leq	\geq
Reflexive	X			X	X
Irreflexive		X	X		
Symmetric	X				
Asymmetric		X	X		
Antisymmetric	X			X	X
Transitive	X	X	X	X	X

Combining Relations

$$R_1 = \{(1,1), (2,2), (3,3)\}$$

$$R_2 = \{(1,1), (1,2), (1,3), (1,4)\}$$

$$R_1 \cup R_2 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (3,3)\}$$

$$R_1 \cap R_2 = \{(1,1)\}$$

$$R_1 - R_2 = \{(2,2), (3,3)\}$$

n-ary relations

An n-ary relation on sets A_1, A_2, \dots, A_n
is a subset of Cartesian product $A_1 \times A_2 \times \dots \times A_n$
The sets A_1, A_2, \dots, A_n are called the domains
of the relation, and n is called its degree.

Example: A relation on $N \times N \times N$

All triples of numbers (a, b, c) with $a < b < c$

$$R = \{(1, 2, 3), (1, 2, 4), (1, 2, 5), \dots\}$$

Relational data model

n-ary relation R is represented with table

fields

R : Teaching assignments

records →

Professor	Department	Course-number
Cruz	Zoology	335
Cruz	Zoology	412
Farber	Psychology	501
Farber	Psychology	617
Rosen	Comp. Science	518
Rosen	Mathematics	575

↑
primary key
(all entries are different)

Selection operator: $s_C(R)$

keeps all records that satisfy condition C

Example: C : Department = Psychology

Result of selection operator $s_C(R)$

Professor	Department	Course-number
Farber	Psychology	501
Farber	Psychology	617

Projection operator: $P_{i_1, i_2, \dots, i_m}(R)$

Keeps only the fields i_1, i_2, \dots, i_m of R

Example:

$P_{\text{Professor, Department}}(R)$

Professor	Department
Cruz	Zoology
Farber	Psychology
Rosen	Comp. Science
Rosen	Mathematics

Join operator: $J_k(R, S)$

Concatenates the records of R and S
where the last k fields of R
are the same with the first k fields of S

S: Class schedule

Department	Course-number	Room	Time
Comp. Science	518	N521	2:00pm
Mathematics	575	N502	3:00pm
Mathematics	611	N521	4:00pm
Psychology	501	A100	3:00pm
Psychology	617	A110	11:00am
Zoology	335	A100	9:00am
Zoology	412	A100	8:00am

$J_2(R,S)$

Professor	Department	Course Number	Room	Time
Cruz	Zoology	335	A100	9:00am
Cruz	Zoology	412	A100	8:00am
Farber	Psychology	501	A100	3:00pm
Farber	Psychology	617	A110	11:00am
Rosen	Comp. Science	518	N521	2:00pm
Rosen	Mathematics	575	N502	3:00pm

Representing Relations with Matrices

$$A = \{a_1, a_2, a_3\}$$

$$B = \{b_1, b_2, b_3, b_4, b_5\}$$

$$R = \{(a_1, b_2), (a_2, b_1), (a_2, b_3), (a_2, b_4), (a_3, b_1), (a_3, b_3), (a_3, b_5)\}$$

Relation Matrix

$$M_R$$

$$B$$

$$A \begin{bmatrix} a_1 & b_1 & b_2 & b_3 & b_4 & b_5 \\ a_2 & 0 & 1 & 0 & 0 & 0 \\ a_3 & 1 & 0 & 1 & 1 & 0 \\ & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Reflexive relation R on set A :

$$\forall a \in A, (a, a) \in R$$

Diagonal elements must be 1

Example: $A = \{1, 2, 3, 4\}$

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

	a_1	a_2	a_3	a_4
a_1	1	1		
a_2	1	1		
a_3			1	1
a_4			1	1

Symmetric relation R : $(a, b) \in R \rightarrow (b, a) \in R$

Matrix is equal to its transpose: $M_R = M_R^T$

Example: $A = \{1, 2, 3, 4\}$

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

For all i, j

$$M_R[i, j] = M_R[j, i]$$

$$\begin{matrix} & a_1 & a_2 & a_3 & a_4 \\ a_1 & \left[\begin{array}{cccc} 1 & 1 & & \\ 1 & 1 & & \\ & & 1 & \\ & & 1 & 1 \end{array} \right] \\ a_2 & & & & \\ a_3 & & & & \\ a_4 & & & & \end{matrix}$$

Antisymmetric relation R :

$$(a, b) \in R \wedge (b, a) \in R \rightarrow a = b$$

Example: $A = \{1, 2, 3, 4\}$

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

For all $i \neq j$

$$M_R[i, j] \neq M_R[j, i]$$

	a_1	a_2	a_3	a_4
a_1	1			
a_2	1	1		
a_3			1	
a_4	1			1

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

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

Union $R \cup S :$ $M_{R \cup S} = M_R \vee M_S = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$

Intersection $R \cap S :$

$$M_{R \cap S} = M_R \wedge M_S = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

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

$$A \cup B = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

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

$$A \cap B = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Composite Relation

- 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 ordered pairs (a, c) , where $a \in A$, $c \in C$, and for which there exists an element $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$.
- We denote the composite of R and S by $S \circ R$.

Composite relation: $S \circ R$

$$(a, b) \in S \circ R \leftrightarrow \exists x : (a, x) \in R \wedge (x, b) \in S$$

Note: $(a, b) \in R \wedge (b, c) \in S \rightarrow (a, c) \in S \circ R$

Example:

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

$$S = \{(1,0), (2,0), (3,1), (3,2), (4,1)\}$$

$$S \circ R = \{(1,0), (1,1), (2,1), (2,2), (3,0), (3,1)\}$$

Combining Relations

• **Example:** Let D and S be relations on $A = \{1, 2, 3, 4\}$.

• $D = \{(a, b) \mid b = 5 - a\}$ “ b equals $(5 - a)$ ”

• $S = \{(a, b) \mid a < b\}$ “ a is smaller than b ”

• $D = \{(1, 4), (2, 3), (3, 2), (4, 1)\}$

• $S = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$

• $S \circ D = \{(2, 4), (3, 3), (3, 4), (4, 2), (4, 3), (4, 4)\}$

D maps an element a to the element $(5 - a)$, and afterwards S maps $(5 - a)$ to all elements larger than $(5 - a)$, resulting in $S \circ D = \{(a, b) \mid b > 5 - a\}$ or $S \circ D = \{(a, b) \mid a + b > 5\}$.

Power of relation: R^n

$$R^1 = R \quad R^{n+1} = R^n \circ R$$

Example: $R = \{(1,1), (2,1), (3,2), (4,3)\}$

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

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

$$R^4 = R^3 \circ R = R^3$$

Theorem: A relation R is transitive if and only if $R^n \subseteq R$ for all $n = 1, 2, 3, \dots$

Proof: 1. If part: $R^2 \subseteq R$

2. Only if part: use induction

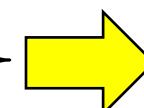
1. If part: We will show that if $R^2 \subseteq R$
then R is transitive

Assumption: $R^2 \subseteq R$

Definition of power: $R^2 = R \circ R$

Definition of composition:

$$(a, b) \in R \wedge (b, c) \in R \rightarrow (a, c) \in R \circ R$$



$$(a, c) \in R$$

Therefore, R is transitive

2. Only if part:

We will show that if R is transitive
then $\underline{R^n \subseteq R}$ for all $n \geq 1$

Proof by induction on n

Inductive basis: $n = 1$

It trivially holds $R^1 = R \subseteq R$

Inductive hypothesis:

Assume that $R^k \subseteq R$

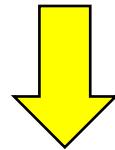
for all $1 \leq k \leq n$

Inductive step: We will prove $R^{n+1} \subseteq R$

Take arbitrary $(a, b) \in R^{n+1}$

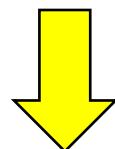
We will show $(a, b) \in R$

$$(a, b) \in R^{n+1}$$



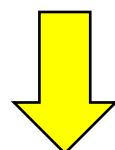
definition of power

$$(a, b) \in R^n \circ R$$



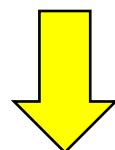
definition of composition

$$\exists x : (a, x) \in R \wedge (x, b) \in R^n$$



inductive hypothesis $R^n \subseteq R$

$$\exists x : (a, x) \in R \wedge (x, b) \in R$$



R is transitive

$$(a, b) \in R$$

End of Proof

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

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

Composition $S \circ R$: Boolean matrix product

$$M_{S \circ R} = M_R \circ M_S = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

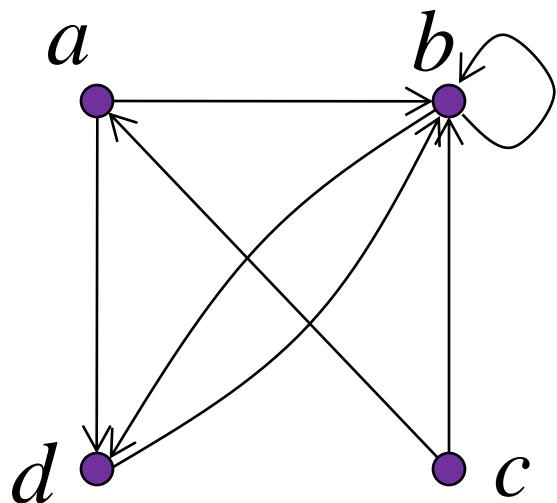
$$M_R = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

Power $R^2 = R \circ R$: Boolean matrix product

$$M_{R^2} = M_R \circ M_R = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

Digraphs (Directed Graphs)

$$R = \{(a,b), (a,d), (b,b), (b,d), (c,a), (c,b), (d,b)\}$$



Theorem: $(a,b) \in R^n$
if and only if
there is a path of length n
from a to b in R

Connectivity relation:

$$R^* = R^1 \cup R^2 \cup R^3 \cup \dots = \bigcup_{i=1}^{\infty} R^i$$

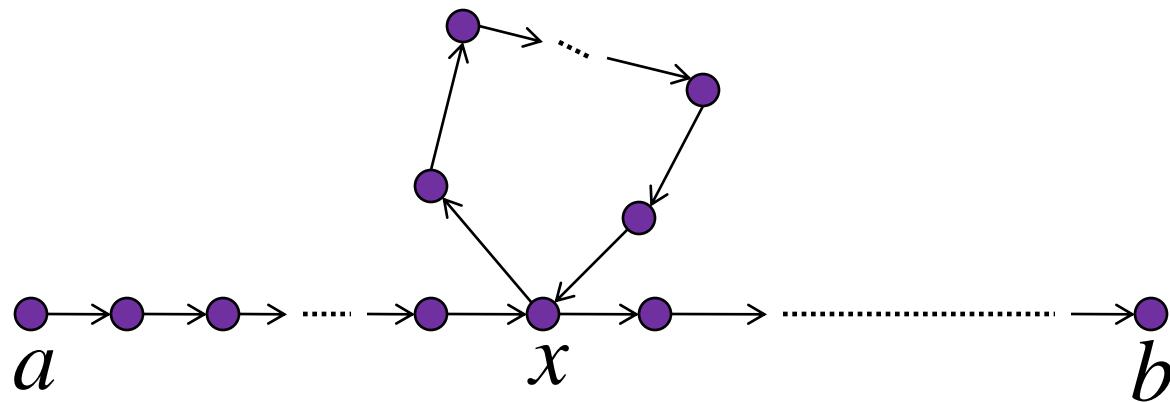
$$(a,b) \in R^*$$

if and only if
there is some path (of any length)
from a to b in R

Theorem:

$$R^* = R^1 \cup R^2 \cup R^3 \cup \dots \cup R^n$$

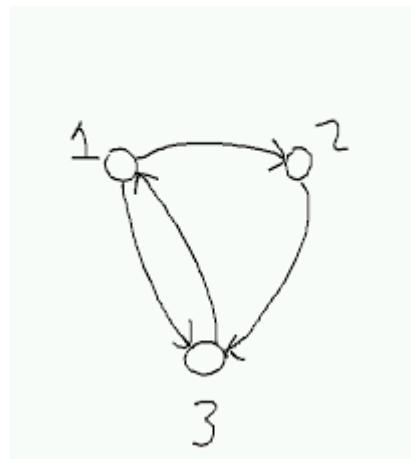
Proof: if $(a,b) \in R^{n+1}$ then $(a,b) \in R^i$
for some $i \in \{1, \dots, n\}$



Repeated node

Example

- Let R be the relation on the set of all people in the world that contains (a, b) if a has met b . What is R^n , where n is a positive integer greater than one? What is R^* ?
- Solution:
 - The relation R^2 contains (a, b) if there is a person c such that $(a, c) \in R$ and $(c, b) \in R$,
 - that is, if there is a person c such that a has met c and c has met b .
 - Similarly, R^n consists of those pairs (a, b) such that there are people x_1, x_2, \dots, x_{n-1} such that a has met x_1 , x_1 has met x_2, \dots , and x_{n-1} has met b .
 - The relation R^* contains (a, b) if there is a sequence of people, starting with a and ending with b , such that each person in the sequence has met the next person in the sequence.



Closures and Relations

Reflexive closure of R :

Smallest size relation that contains R and is reflexive

Easy to find

- The relation $R = \{(1, 1), (1, 2), (2, 1), (3, 2)\}$ on the set $A = \{1, 2, 3\}$ is not reflexive
- To make R reflexive we add $(2, 2)$ and $(3, 3)$ to R ,
- any reflexive relation that contains R must also contain $(2, 2)$ and $(3, 3)$.
- Because this relation contains R , is reflexive, and is contained within every reflexive relation that contains R , it is called the **reflexive closure** of R .

- What is the reflexive closure of the relation $R = \{(a, b) \mid a < b\}$ on the set of integers?
- Solution: The reflexive closure of R is $R^U = \{(a, b) \mid a < b\} \cup \{(a, a) \mid a \in \mathbb{Z}\} = \{(a, b) \mid a \leq b\}$.

Symmetric closure of R :

Smallest size relation that contains R and is symmetric

Easy to find

- $\{(1, 1), (1, 2), (2, 2), (2, 3), (3, 1), (3, 2)\}$ on $\{1, 2, 3\}$ is not symmetric
- we need only add $(2, 1)$ and $(1, 3)$, because these are the only pairs of the form (b, a) with $(a, b) \in R$ that are not in R .
- This new relation is symmetric and contains R .
- new relation is called the **symmetric closure** of R .

- What is the symmetric closure of the relation $R = \{(a, b) \mid a > b\}$ on the set of positive integers?
- *Solution:* The symmetric closure of R is the relation

$$RUR^{-1} = \{(a, b) \mid a > b\} \cup \{(b, a) \mid a > b\} = \{(a, b) \mid a = b\}.$$

$$R \cup R^{-1} = \{(a, b) \mid a > b\} \cup \{(b, a) \mid a > b\} = \{(a, b) \mid a \neq b\}.$$

- What is the symmetric closure of the relation $R = \{(a, b) \mid a > b\}$ on the set of positive integers?
- *Solution:* The symmetric closure of R is the relation

$$RUR^{-1} = \{(a, b) \mid a > b\} \cup \{(b, a) \mid a > b\} = \{(a, b) \mid a = b\}.$$

$$R \cup R^{-1} = \{(a, b) \mid a > b\} \cup \{(b, a) \mid a > b\} = \{(a, b) \mid a \neq b\}.$$

Transitive closure of R :

Smallest size relation that contains R and is transitive

More difficult to find

- $R = \{(1, 3), (1, 4), (2, 1), (3, 2)\}$ on the set $\{1, 2, 3, 4\}$. This relation is not transitive because it does not contain all pairs of the form (a, c) where (a, b) and (b, c) are in R .
- The pairs of this form not in R are $(1, 2)$, $(2, 3)$, $(2, 4)$, and $(3, 1)$. Adding these pairs does not produce a transitive relation, because the resulting relation contains $(3, 1)$ and $(1, 4)$ but does not contain $(3, 4)$. This shows that constructing the transitive closure of a relation is more complicated than constructing either the reflexive or symmetric closure.

Closure

- $(R^+)^{\#} = (R^{\#})^+$
- $(R^*)^+ = (R^+)^*$
- $(R^*)^{\#} = (R^{\#})^*$

R^+ Reflexive closure

$R^{\#}$ Symmetric closure

R^* Transitive Closure

Theorem: R^* is the transitive Closure of R

Proof: Part 1: R^* is transitive

Part 2: If $R \subseteq S$ and S is transitive

Then $R^* \subseteq S^* \subseteq S$

Directed Graph

- 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 the vertex b is called the terminal vertex of this edge.

- a relation is reflexive if and only if there is a loop at every vertex of the directed graph, so that every ordered pair of the form (x, x) occurs in the relation.
- A relation is symmetric if and only if for every edge between distinct vertices in its digraph there is an edge in the opposite direction, so that (y, x) is in the relation whenever (x, y) is in the relation.
- A relation is symmetric if and only if for every edge between distinct vertices in its digraph there is an edge in the opposite direction, so that (y, x) is in the relation whenever (x, y) is in the relation.

Theorem: $(a,b) \in R^n$
if and only if
there is a path of length n
from a to b in R

Connectivity relation:

$$R^* = R^1 \cup R^2 \cup R^3 \cup \dots = \bigcup_{i=1}^{\infty} R^i$$

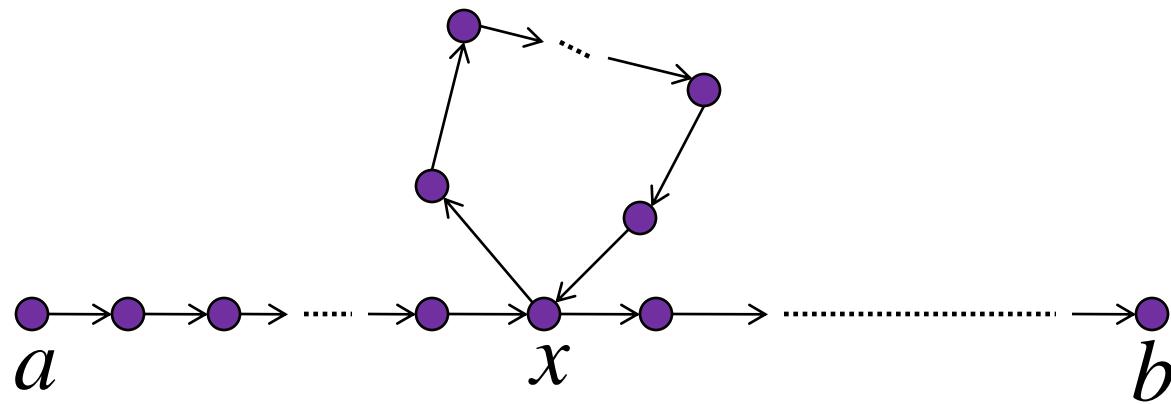
$$(a,b) \in R^*$$

if and only if
there is some path (of any length)
from a to b in R

Theorem:

$$R^* = R^1 \cup R^2 \cup R^3 \cup \dots \cup R^n$$

Proof: if $(a,b) \in R^{n+1}$ then $(a,b) \in R^i$
for some $i \in \{1, \dots, n\}$



Repeated node

Example

- Let R be the relation on the set of all people in the world that contains (a, b) if a has met b . What is R^n , where n is a positive integer greater than one? What is R^* ?
- Solution:
 - The relation R^2 contains (a, b) if there is a person c such that $(a, c) \in R$ and $(c, b) \in R$,
 - that is, if there is a person c such that a has met c and c has met b .
 - Similarly, R^n consists of those pairs (a, b) such that there are people x_1, x_2, \dots, x_{n-1} such that a has met x_1 , x_1 has met x_2, \dots , and x_{n-1} has met b .
 - The relation R^* contains (a, b) if there is a sequence of people, starting with a and ending with b , such that each person in the sequence has met the next person in the sequence.

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 $\mathbf{M}_{R^*} = \mathbf{M}_R \vee \mathbf{M}_R^{[2]} \vee \mathbf{M}_R^{[3]} \vee \dots \vee \mathbf{M}_R^{[n]}$.

Example

- Find the zero-one matrix of the transitive closure of the relation R where

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

By Theorem 3, it follows that the zero-one matrix of R^* is

$$\mathbf{M}_{R^*} = \mathbf{M}_R \vee \mathbf{M}_R^{[2]} \vee \mathbf{M}_R^{[3]}$$

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

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

Algorithm for the transitive closure

procedure *transitive closure* (\mathbf{M}_R : zero–one $n \times n$ matrix)

$\mathbf{A} := \mathbf{M}_R$

$\mathbf{B} := \mathbf{A}$

for $i := 2$ **to** n

$\mathbf{A} := \mathbf{A} \odot \mathbf{M}_R$

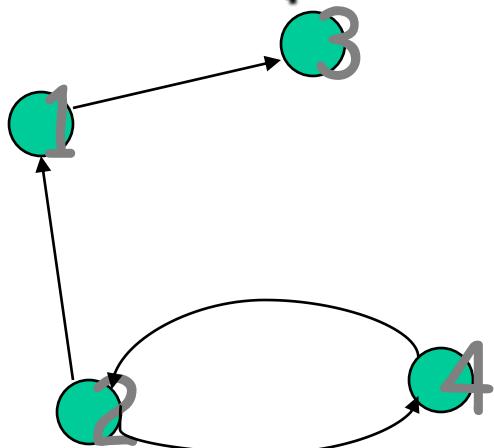
$\mathbf{B} := \mathbf{B} \vee \mathbf{A}$

return \mathbf{B} { \mathbf{B} is the zero–one matrix for R^* }

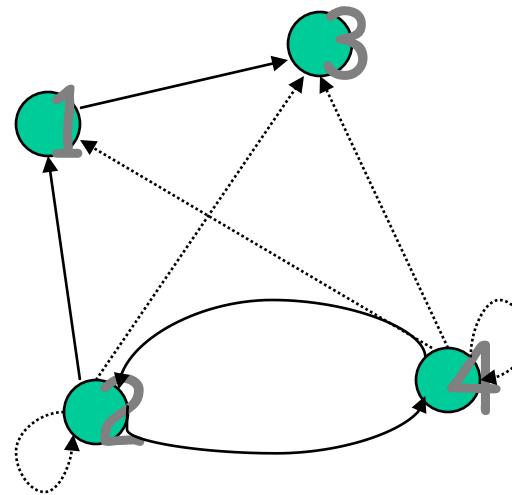
- requires $n-1$.
- Boolean products can be found using *bit operations*
- Hence, these products can be computed using $n^2(2n - 1)(n - 1)$ *bit operations*.
- To find \mathbf{M}_{R^*} need
- Therefore,
- *bit operations needed*

Warshall's algorithm: transitive closure

- Computes the transitive closure of a relation
- (Alternatively: all paths in a directed graph)
- Example of transitive closure:



0	0	1	0
1	0	0	1
0	0	0	0
0	1	0	0



0	0	1	0
1	1	1	1
0	0	0	0
1	1	1	1

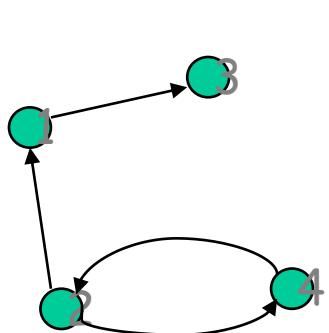
Warshall's algorithm

- Main idea: a path exists between two vertices i, j , iff there is an edge from i to j ;
or
 - there is a path from i to j going through intermediate vertices which are drawn from set {vertex 1}; or
 - there is a path from i to j going through intermediate vertices which are drawn from set {vertex 1, 2}; or
 - ...

Warshall's algorithm

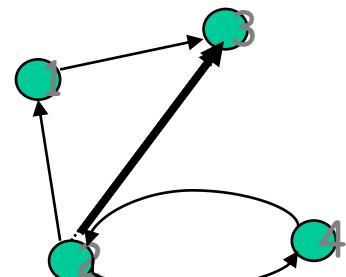
- Main idea: a path exists between two vertices i, j , iff
 - there is a path from i to j going through intermediate vertices which are drawn from set {vertex 1, 2, ... $k-1$ }; or
 - there is a path from i to j going through intermediate vertices which are drawn from set {vertex 1, 2, ... k }; or
 - ...
 - there is a path from i to j going through any of the other vertices

Warshall's algorithm



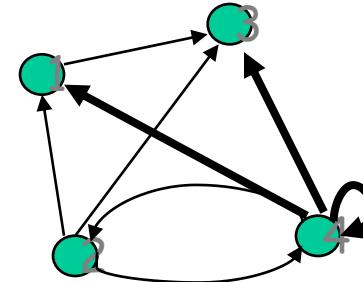
$$R^0$$

0	0	1	0
1	0	0	1
0	0	0	0
0	1	0	0



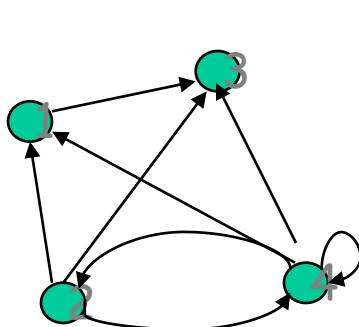
$$R^1$$

0	0	1	0
1	0	1	1
0	0	0	0
0	1	0	0



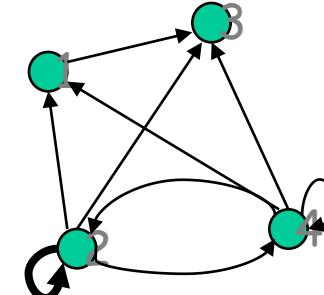
$$R^2$$

0	0	1	0
1	0	1	1
0	0	0	0
1	1	1	1



$$R^3$$

0	0	1	0
1	0	1	1
0	0	0	0
1	1	1	1



$$R^4$$

0	0	1	0
1	1	1	1
0	0	0	0
1	1	1	1

Warshall's algorithm

$R^0 = A$
0 0 1 0
1 0 0 1
0 0 0 0
0 1 0 0

R^1
0 0 1 0
1 0 1 1
0 0 0 0
0 1 0 0

R^2
0 0 1 0
1 0 1 1
0 0 0 0
1 1 1 1

R^3
0 0 1 0
1 0 1 1
0 0 0 0
1 1 1 1

R^4
0 0 1 0
1 1 1 1
0 0 0 0
1 1 1 1

In-class exercises

- Apply Warshall's algorithm to find the transitive closure of the digraph defined by the following adjacency matrix

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

Solution

MR

$$\left[\begin{array}{cccc} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right]$$

MR^2

$$\left[\begin{array}{cccc} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right]$$

MR^3

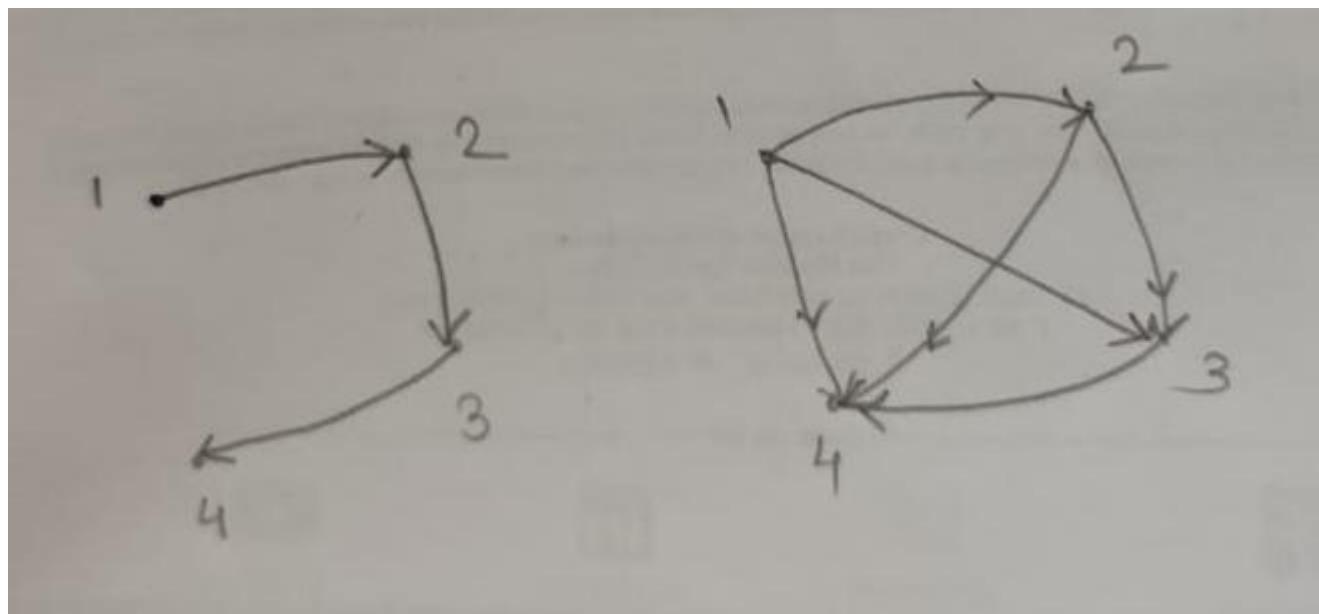
$$\left[\begin{array}{cccc} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right]$$

MR^4

$$\left[\begin{array}{cccc} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right]$$

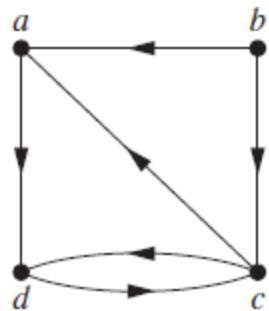
MR^5

$$\left[\begin{array}{cccc} 1 & 0 & 1 & 1 \\ 2 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 \end{array} \right]$$



Let R be the relation with directed graph shown in Figure 3. Let a, b, c, d be a listing of the elements of the set. Find the matrices W_0, W_1, W_2, W_3 , and W_4 . The matrix W_4 is the transitive closure of R .

Let $v_1 = a, v_2 = b, v_3 = c$, and $v_4 = d$. W_0 is the matrix of the
Hence,



$$W_0 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

- W_1 has 1 as its (i, j) th entry if there is a path from v_i to v_j that has only $v_1 = a$ as an interior vertex. Note that all paths of length one can still be used because they have no interior vertices.
- Also, there is now an allowable path from b to d , namely, b, a, d .
Hence,

$$W_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

- W_2 has 1 as its (i, j) th entry if there is a path from v_i to v_j that has only $v_1 = a$ and/or $v_2 = b$ as its interior vertices, if any. Because there are no edges that have b as a terminal vertex, no new paths are obtained when we permit b to be an interior vertex. Hence, $W_2 = W_1$.
- W_3 has 1 as its (i, j) th entry if there is a path from v_i to v_j that has only $v_1 = a$, $v_2 = b$, and/or $v_3 = c$ as its interior vertices, if any. We now have paths from d to a , namely, d, c, a , and from d to d , namely, d, c, d . Hence,

$$W_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}.$$

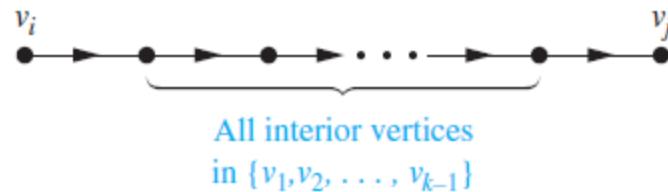
- Finally, W_4 has 1 as its (i, j) th entry if there is a path from v_i to v_j that has $v_1 = a$, $v_2 = b$, $v_3 = c$, and/or $v_4 = d$ as interior vertices, if any. Because these are all the vertices of the graph, this entry is 1 if and only if there is a path from v_i to v_j . Hence,

$$W_4 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}.$$

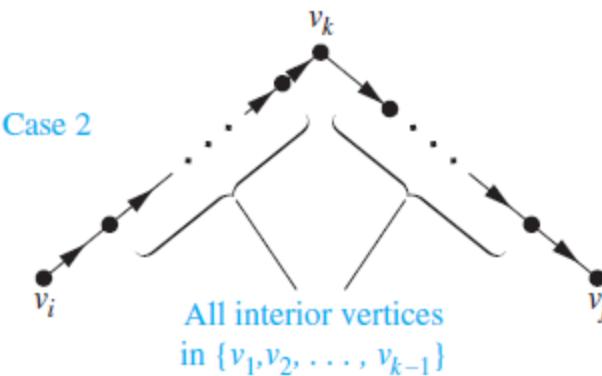
- This last matrix, W_4 , is the matrix of the transitive closure

- The first type of path exists if and only if $w[k-1]ij = 1$, and the second type of path exists if and only if both $w[k-1]ik$ and $w[k-1]kj$ are 1. Hence, $w[k]ij$ is 1 if and only if either $w[k-1]ij$ is 1 or both $w[k-1]ik$ and $w[k-1]kj$ are 1.

Case 1



Case 2



Lemma

Let $\mathbf{W}_k = [w_{ij}^{[k]}]$ be the zero-one matrix that has a 1 in its (i, j) th position if and only if there is a path from v_i to v_j with interior vertices from the set $\{v_1, v_2, \dots, v_k\}$. Then

$$w_{ij}^{[k]} = w_{ij}^{[k-1]} \vee (w_{ik}^{[k-1]} \wedge w_{kj}^{[k-1]}),$$

whenever i , j , and k are positive integers not exceeding n .

procedure *Warshall* ($\mathbf{M}_R : n \times n$ zero-one matrix)

$\mathbf{W} := \mathbf{M}_R$

for $k := 1$ **to** n

for $i := 1$ **to** n

for $j := 1$ **to** n

$w_{ij} := w_{ij} \vee (w_{ik} \wedge w_{kj})$

return $\mathbf{W}\{\mathbf{W} = [w_{ij}] \text{ is } \mathbf{M}_{R^*}\}$

- The computational complexity of Warshall's algorithm can easily be computed in terms of bit operations. To find the entry $w[k]ij$ from the entries $w[k-1]ij$, $w[k-1]ik$, and $w[k-1]kj$ using Lemma requires two bit operations. To find all n^2 entries of \mathbf{W}_k from those of \mathbf{W}_{k-1} requires $2n^2$ bit operations. Because ' $n \cdot 2n^2 = 2n^3$ ' algorithm begins with $\mathbf{W}_0 = \mathbf{M}_R$ and computes the sequence of n zero-one matrices $\mathbf{W}_1, \mathbf{W}_2, \dots, \mathbf{W}_n = \mathbf{M}_{R^*}$, the total number of bit operations used

Which of the following is the transitive closure?

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

a) $\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$

b) $\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$

c) $\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$

Equivalence Relations

Equivalence relations are used to relate objects that are similar in some way.

Definition: A relation on a set A is called an equivalence relation if it is reflexive, symmetric, and transitive.

Two elements that are related by an equivalence relation R are called **equivalent**.

Since R is **symmetric**, a is equivalent to b whenever b is equivalent to a.

Since R is **reflexive**, every element is equivalent to itself.

Since R is **transitive**, if a and b are equivalent and b and c are equivalent, then a and c are equivalent.

Obviously, these three properties are necessary for a reasonable definition of equivalence.

Example: Suppose that R is the relation on the set of strings that consist of English letters such that aRb if and only if $l(a) = l(b)$, where $l(x)$ is the length of the string x . Is R an equivalence relation?

Solution:

- R is reflexive, because $l(a) = l(a)$ and therefore aRa for any string a .
- R is symmetric, because if $l(a) = l(b)$ then $l(b) = l(a)$, so if aRb then bRa .
- R is transitive, because if $l(a) = l(b)$ and $l(b) = l(c)$, then $l(a) = l(c)$, so aRb and bRc implies aRc .

R is an equivalence relation.

Example

- Let R be the relation on the set of real numbers such that aRb if and only if $a - b$ is an integer. Is R an equivalence relation?
- Solution:
 - Because $a - a = 0$ is an integer for all real numbers a , aRa for all real numbers a . Hence, R is reflexive.
 - Now suppose that aRb . Then $a - b$ is an integer, so $b - a$ is also an integer. Hence, bRa . It follows that R is symmetric.
 - If aRb and bRc , then $a - b$ and $b - c$ are integers.
 - Therefore, $a - c = (a - b) + (b - c)$ is also an integer. Hence, aRc . Thus, R is transitive. Consequently, R is an equivalence relation

Equivalence Classes

Definition: Let R be an equivalence relation on a set A . The set of all elements that are related to an element a of A is called the **equivalence class** of a .

The equivalence class of a with respect to R is denoted by $[a]_R$.

When only one relation is under consideration, we will delete the subscript R and write $[a]$ for this equivalence class.

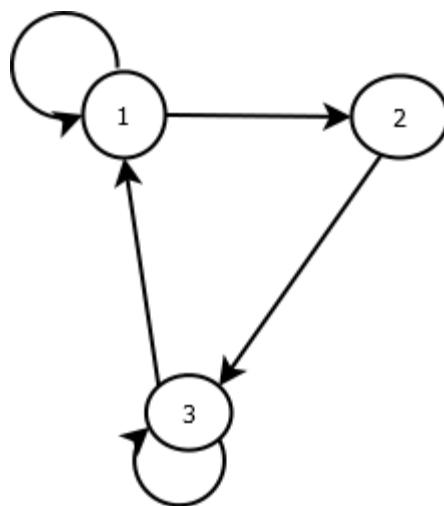
If $b \in [a]_R$, b is called a **representative** of this equivalence class.

Example: In the previous example (strings of identical length), what is the equivalence class of the word mouse, denoted by [mouse] ?

Solution: [mouse] is the set of all English words containing five letters.

For example, 'horse' would be a representative of this equivalence class.

Is the Diagram represents an Equivalence Relation?



Equivalence classes

Theorem: Let R be an equivalence relation on a set

A. The following statements are equivalent:

- aRb
- $[a] = [b]$
- $[a] \cap [b] \neq \emptyset$

Equivalence classes

- **Example:**
- The relation $R=\{(a,b) \mid |a+1|=|b+1|\}$ is defined on the set of integers Z . Find the equivalence classes for R .
- **Solution:**
 - It's easy to make sure that R is an equivalence relation. The equivalence classes of R are defined by the expression $\{-1-n, -1+n\}$, where n is an integer.
 - Below are some examples of the classes E_n for specific values of n and the corresponding pairs of the relation R for each of the classes:

Equivalence classes

$n=0: E_0 = [-1] = \{-1\}, R_0 = \{(-1, -1)\}$

$n=1: E_1 = [-2] = \{-2, 0\}, R_1 = \{(-2, -2), (-2, 0), (0, -2), (0, 0)\}$

$n=2: E_2 = [-3] = \{-3, 1\}, R_2 = \{(-3, -3), (-3, 1), (1, -3), (1, 1)\}$

$n=-2: E_{-2} = [1] = \{1, -3\}, R_{-2} = \{(1, 1), (1, -3), (-3, 1), (-3, -3)\}$

$n=10: E_{10} = [-11] = \{-11, 9\}, R_{10} = \{(-11, -11), (-11, 9), (9, -11), (9, 9)\}$

$n=-10: E_{-10} = [-11] = \{9, -11\}, R_{-10} = \{(9, 9), (9, -11), (-11, 9), (-11, -11)\}$ As it can be seen, $E_2 = E_{-2}$, $E_{10} = E_{-10}$. It follows from here that we can list all equivalence classes for R by using non-negative integers n .

Partition

Definition: 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 ,
 $i \in I$, forms a partition of S if and only if

- (i) $A_i \neq \emptyset$ for $i \in I$
- $A_i \cap A_j = \emptyset$, if $i \neq j$
- $\cup_{i \in I} A_i = S$

Examples: Let S be the set $\{u, m, b, r, o, c, k, s\}$.
Do the following collections of sets partition S ?

$\{\{m, o, c, k\}, \{r, u, b, s\}\}$

yes.

$\{\{c, o, m, b\}, \{u, s\}, \{r\}\}$

no (k is missing).

$\{\{b, r, o, c, k\}, \{m, u, s, t\}\}$

no (t is not in S).

$\{\{u, m, b, r, o, c, k, s\}\}$

yes.

$\{\{b, o, o, k\}, \{r, u, m\}, \{c, s\}\}$

yes ($\{b, o, o, k\} = \{b, o, k\}$).

$\{\{u, m, b\}, \{r, o, c, k, s\}, \emptyset\}$

no (\emptyset not allowed).

- **Congruence Modulo m** Let m be an integer with $m > 1$. Show that the relation $R = \{(a, b) \mid a \equiv b \pmod{m}\}$ is an equivalence relation on the set of integers
 - $a \equiv b \pmod{m}$ if and only if m divides $a - b$. Note that $a - a = 0$ is divisible by m , because $0 = 0 \cdot m$. Hence, $a \equiv a \pmod{m}$, so congruence modulo m is **reflexive**.
 - suppose that $a \equiv b \pmod{m}$. Then $a - b$ is divisible by m , so $a - b = km$, where k is an integer. It follows that $b - a = (-k)m$, so $b \equiv a \pmod{m}$. Hence, congruence modulo m is symmetric.
 - Next, suppose that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$.
 - Then m divides both $a - b$ and $b - c$. Therefore, there are integers k and l with $a - b = km$ and $b - c = lm$.
 - Adding these two equations shows that $a - c = (a - b) + (b - c) = km + lm = (k + l)m$. Thus, $a \equiv c \pmod{m}$. Therefore, congruence modulo m is transitive.

Equivalence Class

- What are the equivalence classes of 0 and 1 for congruence modulo 4?
 - equivalence class of 0 contains all integers a such that $a \equiv 0 \pmod{4}$. The integers in this class are those divisible by 4. Hence, the equivalence class of 0 for this relation is

$$[0] = \{\dots, -8, -4, 0, 4, 8, \dots\}.$$

- The equivalence class of 1 contains all the integers a such that $a \equiv 1 \pmod{4}$. The integers in this class are those that have a remainder of 1 when divided by 4. Hence, the equivalence class of 1 for this relation is

$$[1] = \{\dots, -7, -3, 1, 5, 9, \dots\}.$$

- let $n = 3$ and let S be the set of all bit strings. Then $sR3 t$ either when $s = t$ or both s and t are bit strings of length 3 or more that begin with the same three bits. For instance, $01 R_3 01$ and $00111 R_3 00101$, but $01 \cancel{R_3} 010$ and $01011 \cancel{R_3} 01110$. Show that for every set S of strings and every positive integer n , R_n is an equivalence relation on S .
 - The relation R_n is reflexive because $s = s$, so that $sR_n s$ whenever s is a string in S .
 - If $s R_n t$, then either $s = t$ or s and t are both at least n characters long that begin with the same n characters.

$t R_n S \therefore R_n$ is symmetric.

- suppose that $s R_n t$ and $t R_n u$.
- Then either $s = t$ or s and t are at least n characters long and s and t begin with the same n characters,
- And either $t = u$ or t and u are at least n characters long and t and u begin with the same n characters.
- From this, either $s = u$ or both s and u are n characters long and s and u begin with the same n characters
- Consequently, R_n is transitive.
- It follows that R_n is an equivalence relation.

- What is the equivalence class of the string 0111 with respect to the equivalence relation R_3 from on the set of all bit strings? (Recall that $sR_3 t$ if and only if s and t are bit strings with $s = t$ or s and t are strings of at least three bits that start with the same three bits.)
 - The bit strings equivalent to 0111 are the bit strings with at least three bits that begin with 011. These are the bit strings 011, 0110, 0111, 01100, 01101, 01110, 01111, and so on.
 - Consequently, $[011] R_3 = \{011, 0110, 0111, 01100, 01101, 01110, 01111, \dots\}$.

Introduction

- An equivalence relation is a relation that is reflexive, symmetric, and transitive
- A partial ordering (or partial order) is a relation that is reflexive, *antisymmetric*, and transitive
 - Recall that antisymmetric means that if $(a,b) \in R$, then $(b,a) \notin R$ unless $b = a$
 - Thus, (a,a) is allowed to be in R
 - But since it's reflexive, all possible (a,a) must be in R

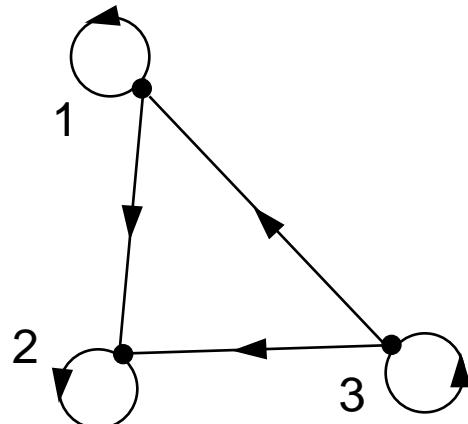
Partially Ordered Set (POSET)

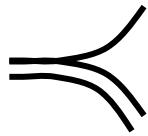
A relation R on a set S is called a *partial ordering* or *partial order* if it is *reflexive*, *antisymmetric*, and *transitive*. A set S together with a partial ordering R is called a *partially ordered set*, or *poset*, and is denoted by (S, R)

Example (1)

Let $S = \{1, 2, 3\}$ and

let $R = \{(1,1), (2,2), (3,3), (1, 2), (3,1), (3,2)\}$





In a poset the notation $a \preccurlyeq b$ denotes that

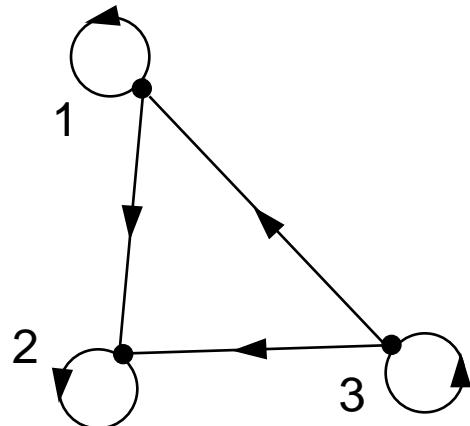
- **(a,b) belong to R**

This notation is used because the “**less than or equal to**” relation is a paradigm for a partial ordering. (Note that the symbol \preccurlyeq is used to denote the relation in *any* poset, not just the “less than or equals” relation.) The notation $a \prec b$ denotes that $a \preccurlyeq b$, but “**a not equal to b**”

Example

Let $S = \{1, 2, 3\}$ and

let $R = \{(1,1), (2,2), (3,3), (1, 2), (3,1), (3,2)\}$



$$2 \preccurlyeq 2$$

$$3 \prec 2$$

Example (2)

- Show that \geq is a partial order on the set of integers
 - It is reflexive: $a \geq a$ for all $a \in \mathbb{Z}$
 - It is antisymmetric: if $a \geq b$ then the only way that $b \geq a$ is when $b = a$
 - It is transitive: if $a \geq b$ and $b \geq c$, then $a \geq c$
- Note that \geq is the partial ordering on the set of integers
- (\mathbb{Z}, \geq) is the partially ordered set, or poset

Example (3)

Consider the power set of $\{a, b, c\}$ and the subset relation.

Comparable / Incomparable

The elements a and b of a poset (S, \preccurlyeq) are called *comparable* if either $a \preccurlyeq b$ or $b \preccurlyeq a$.

When a and b are elements of S such that neither $a \preccurlyeq b$ nor $b \preccurlyeq a$, a and b are called *incomparable*.

Totally Ordered, Chains

If (S, \preccurlyeq) is a poset and every two elements of S are comparable, S is called *totally ordered* or *linearly ordered* set, and \preccurlyeq is called a *total order* or a *linear order*. A totally ordered set is also called a *chain*.

- In the poset (\mathbb{Z}^+, \leq) , are the integers 3 and 9 comparable?
 - Yes, as $3 \leq 9$
- Are 7 and 5 comparable?
 - Yes, as $5 \leq 7$
- As all pairs of elements in \mathbb{Z}^+ are comparable, the poset (\mathbb{Z}^+, \leq) is a total order
 - totally ordered poset, linear order, or chain

- In the poset $(\mathbb{Z}^+, |)$ with “divides” operator $|$, are the integers 3 and 9 comparable?
 - Yes, as $3 \mid 9$
- Are 7 and 5 comparable?
 - No, as $7 \nmid 5$ and $5 \nmid 7$
- Thus, as there are pairs of elements in \mathbb{Z}^+ that are not comparable, the poset $(\mathbb{Z}^+, |)$ is a partial order. It is not a chain.

Hasse Diagrams

Given any partial order relation defined on a finite set, it is possible to draw the directed graph so that all of these properties are satisfied.

This makes it possible to associate a somewhat simpler graph, called a *Hasse diagram*, with a partial order relation defined on a finite set.

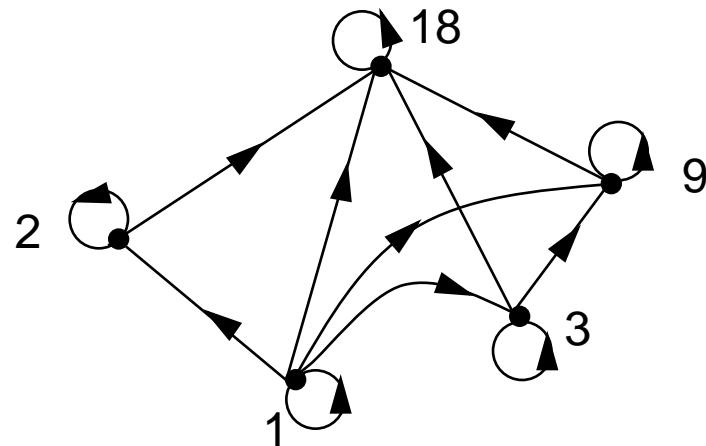
Hasse Diagrams (continued)

Start with a directed graph of the relation in which all arrows point upward. Then eliminate:

1. the loops at all the vertices,
2. all arrows whose existence is implied by the transitive property,
3. the direction indicators on the arrows.

Example

Let $A = \{1, 2, 3, 9, 18\}$ and consider the “divides” relation on A :

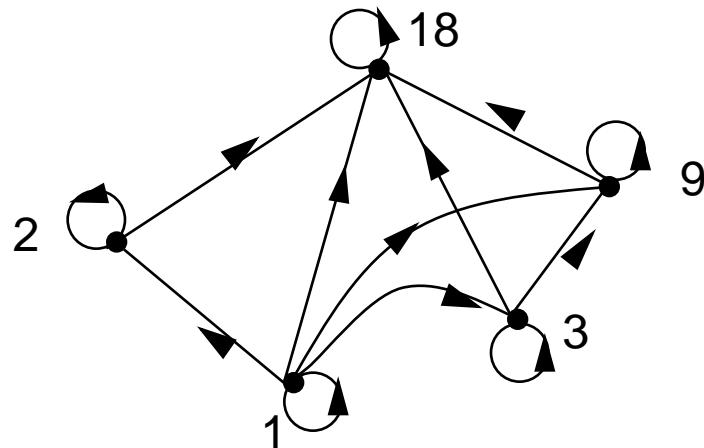


Example

Eliminate the loops at all the vertices.

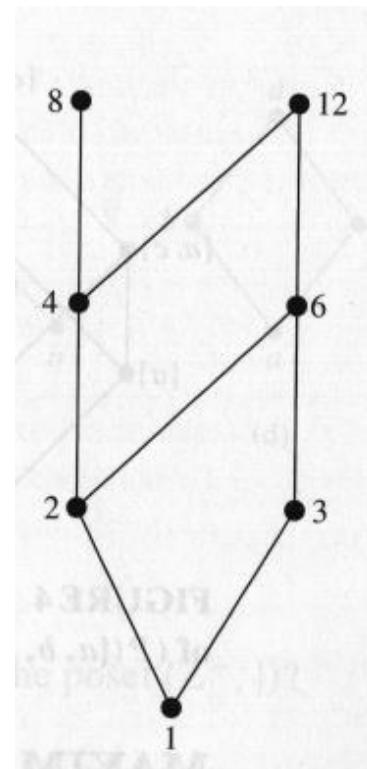
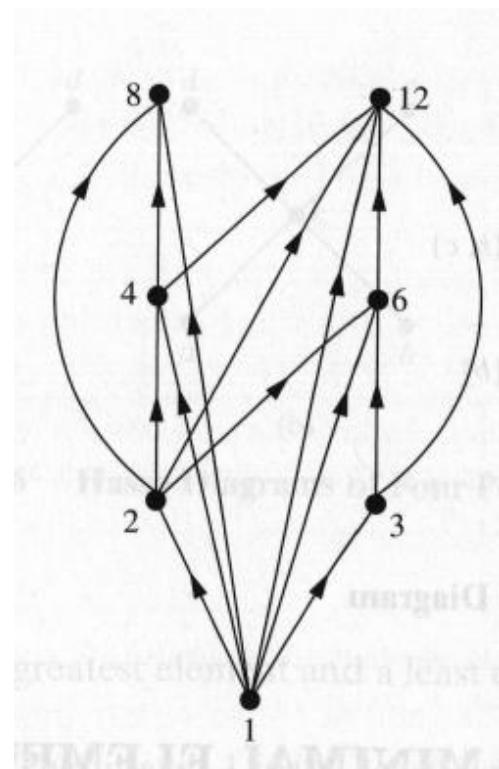
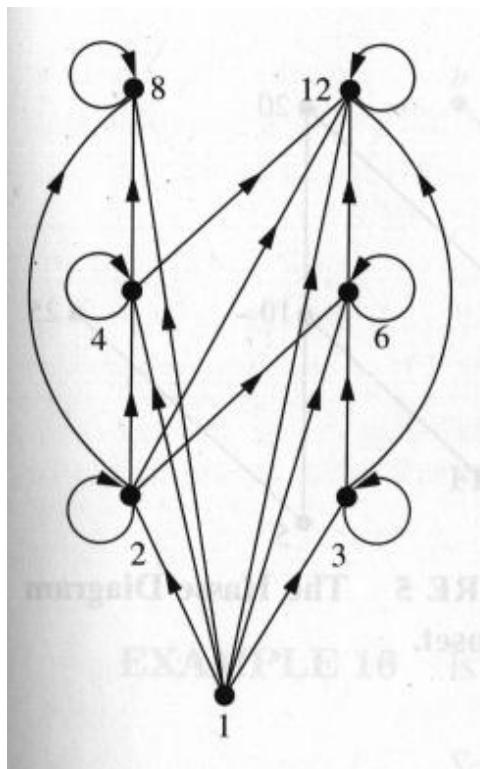
Eliminate all arrows whose existence is implied by the transitive property.

Eliminate the direction indicators on the arrows.



Hasse Diagram

- For the poset $(\{1,2,3,4,6,8,12\}, |)$



Construct the Hasse diagram of $(P(\{a, b, c\}), \subseteq)$.

The elements of $P(\{a, b, c\})$ are

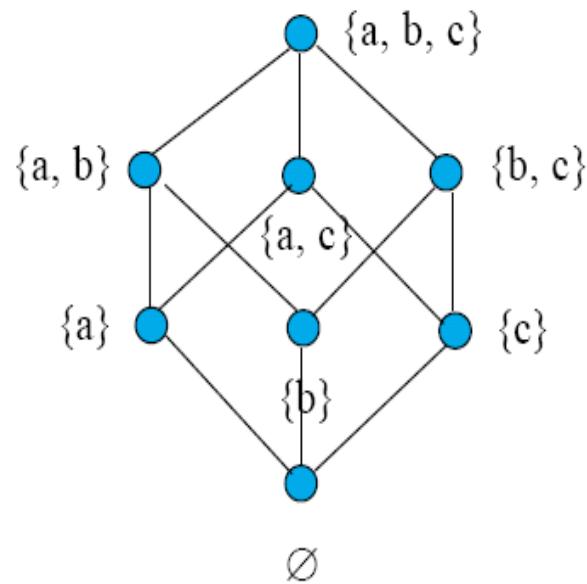
\emptyset

$\{a\}, \{b\}, \{c\}$

$\{a, b\}, \{a, c\}, \{b, c\}$

$\{a, b, c\}$

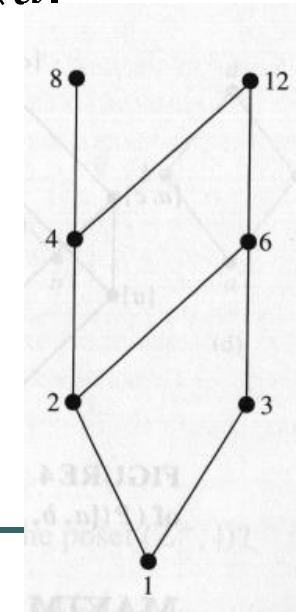
The digraph is



Maximal and Minimal Elements

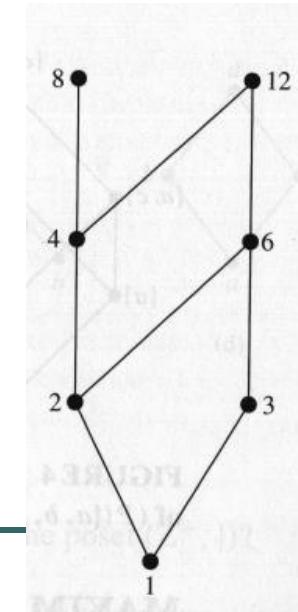
a is a *maximal* in the poset (S, \preceq) if there is no b belonging to S such that $a \prec b$. Similarly, an element of a poset is called *minimal* if it is not greater than any element of the poset. That is, a is *minimal* if there is no element b belonging to S such that $b \prec a$.

It is possible to have
multiple minimals and maximals.



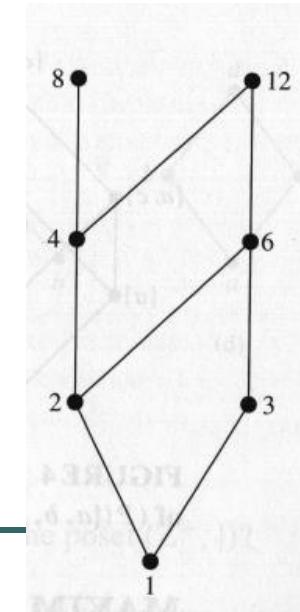
Greatest Element Least Element

a is the *greatest element* in the poset (S, \preccurlyeq) if $b \preccurlyeq a$ for all b belonging to S . Similarly, an element of a poset is called the *least element* if it is less or equal than all other elements in the poset. That is, a is the *least element* if $a \preccurlyeq b$ for all b belonging to S .



Greatest Element Least Element

a is the *greatest element* in the poset (S, \preccurlyeq) if $b \preccurlyeq a$ for all b belonging to S . Similarly, an element of a poset is called the *least element* if it is less or equal than all other elements in the poset. That is, a is the *least element* if $a \preccurlyeq b$ for all b belonging to S .



Upper bound, Lower bound

Sometimes it is possible to find an element that is greater than or = all the elements in a subset A of a poset (S, \preceq) . If u is an element of S such that $a \preceq u$ for all elements a belongs to A , then u is called an *upper bound* of A . Likewise, there may be an element less than all the elements in A . If l is an element of S such that $l \preceq a$ for all elements a belongs to A , then l is called a *lower bound* of A .

Least Upper Bound, Greatest Lower Bound

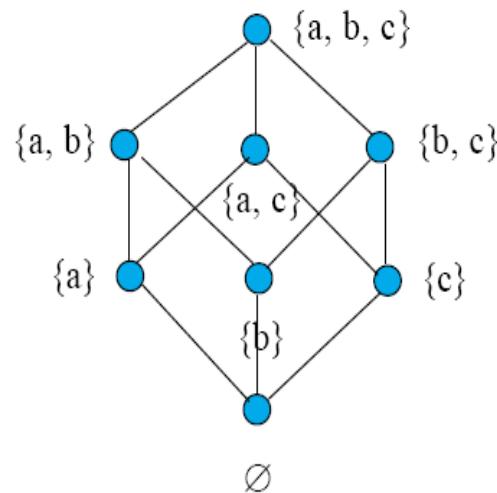
The element x is called the *least upper bound* (lub) of the subset A if x is an upper bound that is less than every other upper bound of A .

The element y is called the *greatest lower bound* (glb) of A if y is a lower bound of A and $z \leq y$ whenever z is a lower bound of A .

Lattices

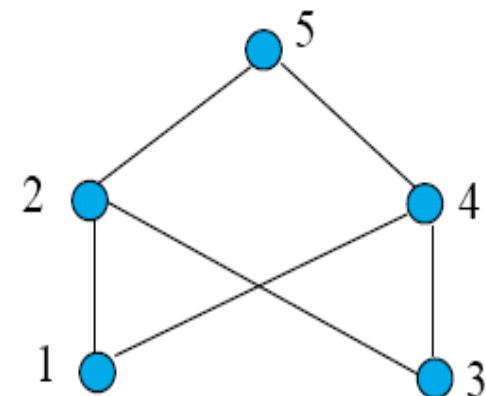
A partially ordered set in which *every pair* of elements has both a least upper bound and a greatest lower bound is called a *lattice*.

$$(P(\{a, b, c\}), \subseteq)$$



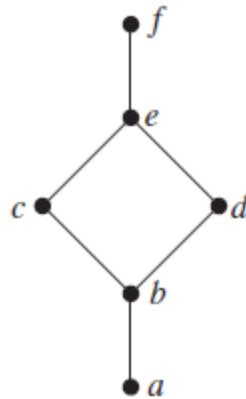
Consider the elements 1 and 3.

- Upper bounds of 1 are 1, 2, 4 and 5.
- Upper bounds of 3 are 3, 2, 4 and 5.
- 2, 4 and 5 are upper bounds for the pair 1 and 3.
- There is no lub since
 - 2 is not related to 4
 - 4 is not related to 2
 - 2 and 4 are both related to 5.
- There is no glb either.

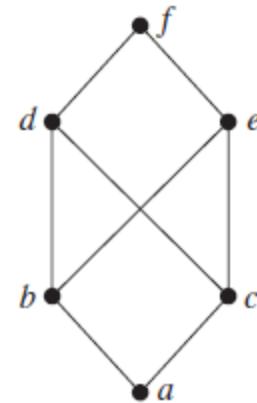


The poset is not a lattice.

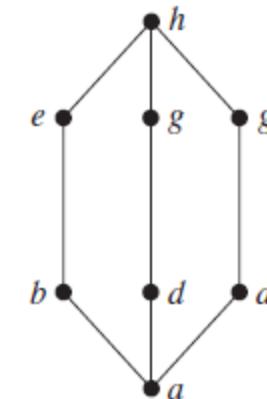
Which of the following are Lattices



(a)

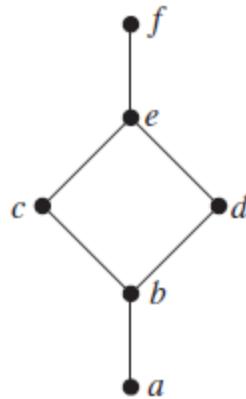


(b)

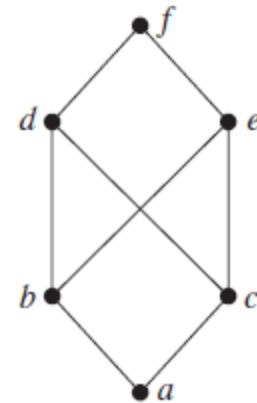


(c)

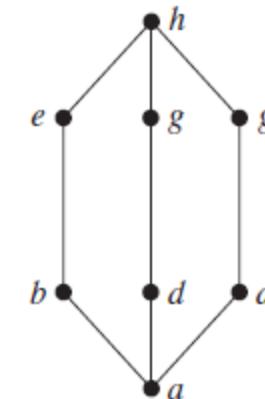
Which of the following are Lattices



(a)



(b)



(c)

- The posets represented by the Hasse diagrams in (a) and (c) are both lattices because in each poset every pair of elements has both a least upper bound and a greatest lower bound, as the reader should verify. On the other hand, the poset with the Hasse diagram shown in (b) is not a lattice, because the elements *b* and *c* have no least upper bound. To see this, note that each of the elements *d*, *e*, and *f* is an upper bound, but none of these three elements precedes the other two with respect to the ordering of this poset.

-
- Determine whether the posets $(\{1, 2, 3, 4, 5\}, |)$ and $(\{1, 2, 4, 8, 16\}, |)$ are lattices.

- Determine whether the posets $(\{1, 2, 3, 4, 5\}, \mid)$ and $(\{1, 2, 4, 8, 16\}, \mid)$ are lattices.

Solution: Because 2 and 3 have no upper bounds in $(\{1, 2, 3, 4, 5\}, \mid)$, they certainly do not have a least upper bound. Hence, the first poset is not a lattice.

- Every two elements of the second poset have both a least upper bound and a greatest lower bound. The least upper bound of two elements in this poset is the larger of the elements and the greatest lower bound of two elements is the smaller of the elements, as the reader should verify.
- Hence, this second poset is a lattice.

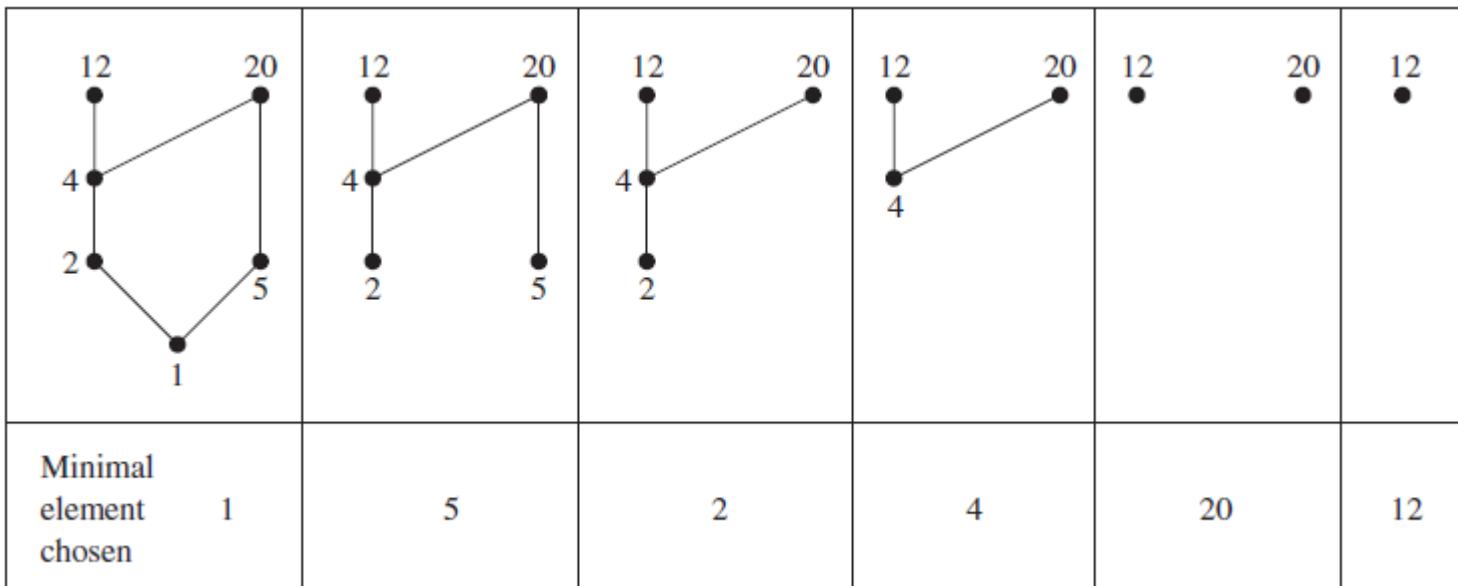
Topological Sorting

- a project is made up of 20 different tasks
- Some tasks can be completed only after others have been finished.
- we set up a partial order on the set of tasks so that $a < b$ if and only if a and b are tasks where b cannot be started until a has been completed.
- To produce a schedule for the project, we need to produce an order for all 20 tasks that is compatible with this partial order

- We begin with a definition. A total ordering \leq is said to be **compatible** with the partial ordering R if $a \leq b$ whenever aRb . Constructing a compatible total ordering from a partial ordering is called **topological sorting**.
- Topological sorting has an application to the scheduling of projects.
- Lemma: Every finite nonempty poset (S, \leq) has at least one minimal element.

Example

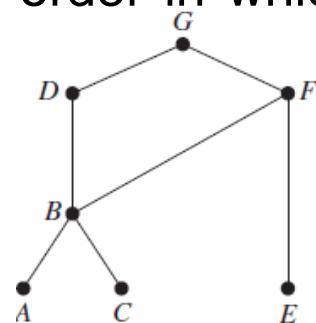
- Find a compatible total ordering for the poset $(\{1, 2, 4, 5, 12, 20\}, |)$.



$$1 \prec 5 \prec 2 \prec 4 \prec 20 \prec 12.$$

- A development project at a computer company requires the completion of seven tasks. Some of these tasks can be started only after other tasks are finished. A partial ordering on tasks is set up by considering task $X < Y$ if task Y cannot be started until task X has been completed.

- The Hasse diagram for the seven tasks, with respect to this partial ordering, is shown in Figure Find an order in which these tasks can be carried out to complete the project.



Minimal element chosen A	C	B	E	F	D	G

Solving Recurrence Relations

A recurrence relation is an equation that recursively defines a sequence where the next term is a function of the previous terms (Expressing F_n as some combination of F_i with $i < n$).

How to solve linear recurrence relation

Homogeneous Recurrence Relations

- Suppose, a two ordered linear recurrence relation is $F_n = AF_{n-1} + BF_{n-2}$
 - where A and B are real numbers.
- The characteristic equation for the above recurrence relation is –
$$x^2 - Ax - B = 0$$
- Three cases may occur while finding the roots –
- **Case 1** – If this equation factors as $(x - x_1)(x - x_2) = 0$ and it produces two distinct real roots x_1 and x_2 , then $F_n = ax_1^n + bx_2^n$ is the solution. [Here, a and b are constants]
- **Case 2** – If this equation factors as $(x - x_1)^2$ and it produces single real root x_1 , then $F_n = ax_1^n + bn x_1^n$ is the solution.
- **Case 3** – If the equation produces two distinct complex roots, x_1 and x_2 in polar form $x_1 = r\angle\Theta$ and $x_2 = r\angle(-\Theta)$, then following is the solution

$$F_n = r^n(a \cos(n\theta) + b \sin(n\theta))$$

Problem 1

Solve the recurrence relation $F_n = 5F_{n-1} - 6F_{n-2}$
where $F_0 = 1$ and $F_1 = 4$

Solution

- The characteristic equation of the recurrence relation is – $x^2 - 5x + 6 = 0$

$$\text{So, } (x-3)(x-2) = 0$$

Hence, the roots are –

$$x_1 = 3$$

$$\text{and } x_2 = 2$$

The roots are real and distinct. So, this is in the form of case 1

- Hence, the solution is –

$$F_n = ax_1^n + bx_2^n$$

- Here, $F = a3^n + b2^n$ (As $x_1=3$ and $x_2=2$)
- Therefore,

$$1 = F_0 = a3^0 + b2^0 = a + b$$

$$4 = F_1 = a3^1 + b2^1 = 3a + 2b$$

- Solving these two equations, we get $a=2$ and $b=-1$
- Hence, the final solution is –

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

Problem 2

Solve the recurrence relation $F_n = 10F_{n-1} - 25F_{n-2}$

where $F_0 = 3$ and $F_1 = 17$

- **Solution**
- The characteristic equation of the recurrence relation is –
$$x^2 - 10x - 25 = 0$$
- So $(x - 5)^2 = 0$
- Hence, there is single real root $x_1 = 5$
- As there is single real valued root, this is in the form of case 2
- Hence, the solution is –
$$F_n = ax_1^n + bnx_1^n$$
- $3 = F_0 = a \cdot 5^0 + b \cdot 5^0 \quad \& \quad 17 = F_1 = a \cdot 5^1 + b \cdot 1 \cdot 5^1$
- Solving these two equations, we get $a=3$
- and $b=2/5$
- Hence, the final solution is $F_n = 3 \cdot 5^n + (2/5) \cdot n \cdot 2^n$

Problem 3

Solve the recurrence relation $F_n = 2F_{n-1} - 2F_{n-2}$

where $F_0 = 1$ and $F_1 = 3$

- **Solution**

- The characteristic equation is $x^2 - 2x - 2 = 0$
Hence, the roots are – $x_1 = 1+i$ and $x_2 = 1-i$
- In polar form, $x_1 = r\angle\theta$ And $x_2 = r\angle(-\theta)$
where $r = \sqrt{2}$ and $\theta = \frac{\pi}{4}$

- The roots are imaginary. So, this is in the form of case 3.

- Hence,
$$F_n = (\sqrt{2})^n (a \cos(n \cdot \frac{\pi}{4}) + b \sin(n \cdot \frac{\pi}{4}))$$
$$1 = F_0 = (\sqrt{2})^0 (a \cos(0 \cdot \frac{\pi}{4}) + b \sin(0 \cdot \frac{\pi}{4})) = a$$
$$3 = F_1 = (\sqrt{2})^1 (a \cos(1 \cdot \frac{\pi}{4}) + b \sin(1 \cdot \frac{\pi}{4})) = \sqrt{2}(a/\sqrt{2} + b\sqrt{2})$$

Solving these two equations we get $a=1$ and $b=2$

- Hence, the final solution is –

$$F_n = (\sqrt{2})^n (\cos(n \cdot \frac{\pi}{4}) + 2 \sin(n \cdot \frac{\pi}{4}))$$

Example: Fibonacci sequence

$$f_n = f_{n-1} + f_{n-2}$$

$$f_0 = 0, \quad f_1 = 1$$

Has solution: $f_n = \lambda_1 r_1^n + \lambda_2 r_2^n$

Characteristic roots:

$$r_1 = \frac{1+\sqrt{5}}{2} \qquad r_2 = \frac{1-\sqrt{5}}{2}$$

$$\lambda_1 = \frac{f_1 - f_0 r_2}{r_1 - r_2} = \frac{1}{\sqrt{5}}$$

$$\lambda_2 = \frac{f_0 r_1 - f_1}{r_1 - r_2} = -\frac{1}{\sqrt{5}}$$

$$f_n = \lambda_1 r_1^n + \lambda_2 r_2^n$$

$$= \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2} \right)^n$$

Non-homogeneous Recurrence Relations

$$F_n = AF_{n-1} + BF_{n-2} + f(n) \text{ where } f(n) \neq 0$$

Its associated homogeneous recurrence relation is $F_n = AF_{n-1} + BF_{n-2}$

The solution (a_n) of a non-homogeneous recurrence relation has two parts.

First part is the solution (a_h) of the associated homogeneous recurrence relation and the second part is the particular solution (a_t) .

$$a_n = a_h + a_t$$

Solution to the first part is done using the procedures discussed in the previous section.

To find the particular solution, we find an appropriate trial solution.

Let $f(n) = cx^n$; let $x^2 = Ax + B$ be the characteristic equation of the associated homogeneous recurrence relation and let x_1 and x_2 be its roots.

- If $x \neq x_1$ and $x \neq x_2$, then $a_t = Ax^n$
- If $x = x_1$, $x \neq x_2$, then $a_t = Anx^n$
- If $x = x_1 = x_2$, then $a_t = An^2x^n$

$$a_n = 5a_{n-1} - 6a_{n-2} + 7^n.$$

- This is a linear nonhomogeneous recurrence relation. The solutions of its associated homogeneous recurrence relation $a_n = 5a_{n-1} - 6a_{n-2}$

Are $a_n^{(h)} = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n$, where α_1 and α_2 are constants

- Because $F(n) = 7^n$, a reasonable trial solution is

$$a_n^{(p)} = C \cdot 7^n,$$

where C is a constant. Substituting the terms of this sequence into the recurrence relation implies that $C \cdot 7^n = 5C \cdot 7^{n-1} - 6C \cdot 7^{n-2} + 7^n$.

- Factoring out 7^{n-2} this equation becomes $49C = 35C - 6C + 49$,
- which implies that $20C = 49$ $C = 49/20$.
- Hence, $a_n^{(p)} = (49/20)7^n$ Is a particular solution,
- All solutions are of the form.

$$a_n = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n + (49/20)7^n.$$

Counting Functions

How many functions are there from a set with m elements to a set with n elements?

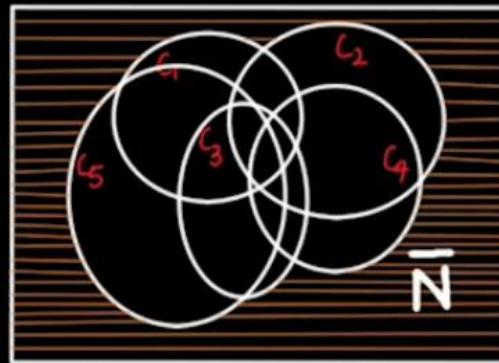
- *Solution:* A function corresponds to a choice of one of the n elements in the codomain for each of the m elements in the domain. Hence, by the product rule there are $n, n, n, \dots, n = n^m$ functions from a set with m elements to one with n elements.
- For example, there are $5^3 = 125$ different functions from a set with three elements to a set with five elements.

Counting One-to-One Functions

How many one-to-one functions are there from a set with m elements to one with n elements?

- First note that when $m > n$ there are no one-to-one functions from a set with m elements to a set with n elements.
- Now let $m \leq n$. Suppose the elements in the domain are a_1, a_2, \dots, a_m . There are n ways to choose the value of the function at a_1 . Because the function is one-to-one, the value of the function at a_2 can be picked in $n - 1$ ways (because the value used for a_1 cannot be used again).
- In general, the value of the function at a_k can be chosen in $n - k + 1$ ways.
- By the product rule, there are $n(n - 1)(n - 2) \cdots (n - m + 1)$ one-to-one functions from a set with m elements to one with n elements.
- For example, there are $5 \cdot 4 \cdot 3 = 60$ one-to-one functions from a set with three elements to a set with five elements.

Total number of graphs in which no one vertex is isolated



$$\begin{aligned}\bar{N} = N - & \left[N(c_1) + N(c_2) + N(c_3) + N(c_4) + N(c_5) \right] + N(c_1c_2) + N(c_1c_3) \\ & + N(c_1c_4) + N(c_1c_5) + N(c_2c_3) + N(c_2c_4) + N(c_2c_5) + N(c_3c_4) \\ & + N(c_3c_5) + N(c_4c_5) - \left[N(c_1c_2c_3) + N(c_1c_2c_4) + N(c_1c_2c_5) \right. \\ & \left. + \dots + N(c_3c_4c_5) \right] + N(c_1c_2c_3c_4) + N(c_1c_2c_3c_5) + N(c_1c_2c_4c_5) \\ & + \dots + N(c_2c_3c_4c_5) - N(c_1c_2c_3c_4c_5)\end{aligned}$$

Number Theory

Divisibility and Modular Arithmetic

Division

- **Definition:** If a and b are integers with $a \neq 0$, then a divides b if there exists an integer c such that $b = ac$.
 - 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 .
 - If $a \mid b$, then b/a is an integer.
 - If a does not divide b , we write $a \nmid b$.

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

Properties of Divisibility

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

- i. If $a | b$ and $a | c$, then $a | (b + c)$;
- ii. If $a | b$, then $a | bm$ for all integers m ;
- iii. If $a | b$ and $b | c$, then $a | c$.

Proof: (i) Suppose $a | b$ and $a | c$, then it follows that there are integers s and t with $b = as$ and $c = at$. Hence,

$$b + c = as + at = a(s + t). \text{ Hence, } a | (b + c)$$

Corollary: If a , b , and c are integers, where $a \neq 0$, such that $a | b$ and $a | c$, then $a | mb + nc$ whenever m and n are integers.

Division Algorithm

- When an integer is divided by a positive integer, there is a quotient and a remainder.
- Division Algorithm:** If a is an integer and d a positive integer, then there are unique integers q and r , with $0 \leq r < d$, such that $a = dq + r$

- d is called the *divisor*.
- a is called the *dividend*.
- q is called the *quotient*.
- r is called the *remainder*.

div and mod

- 1) $q = a \text{ div } d$
- 2) $r = a \text{ mod } d$

Examples:

- What are the quotient and remainder when 101 is divided by 11?

Solution: The quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$, and the remainder is $2 = 101 \text{ mod } 11$.

- What are the quotient and remainder when -11 is divided by 3?

Solution: we have , $-11 = 3(-4) + 1$.

The quotient when -11 is divided by 3 is $-4 = -11 \text{ div } 3$, and the remainder is $1 = -11 \text{ mod } 3$.

Congruence Relation

- ➊ **Definition:** If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$.
 - The notation $a \equiv b \pmod{m}$ says that a is congruent to b modulo m .
 - We say that $a \equiv b \pmod{m}$ is a *congruence* and that m is its *modulus*.
 - Two integers are congruent mod m if and only if they have the same remainder when divided by m .
 - If a is not congruent to b modulo m , we write

$$a \not\equiv b \pmod{m}$$

Example: Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution:

- $17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$.
- $24 \not\equiv 14 \pmod{6}$ since 6 divides $24 - 14 = 10$ is not divisible by 6.

More on Congruence

- **Theorem :** 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 (by the definition of congruence) $m \mid a - b$. Hence, there is an integer k such that $a - b = km$ and equivalently $a = b + km$.
- Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, $m \mid a - b$ and $a \equiv b \pmod{m}$.

The Relationship between $(\text{mod } m)$ and $\text{mod } m$ Notations

- The use of “mod” in $a \equiv b \ (\text{mod } m)$ is different from its use in $a \text{ mod } m = b$.
 - $a \equiv b \ (\text{mod } m)$ is a relation on the set of integers.
 - In $a \text{ mod } m = b$, the notation **mod** denotes a function.
- **Theorem :**

Let a and b be integers, and let m be a positive integer. Then $a \equiv b \ (\text{mod } m)$ if and only if $a \text{ mod } m = b \text{ mod } m$.

Congruences of Sums and Products

- **Theorem :** Let m be a positive integer. If $a \equiv b \pmod{m}$ and

$c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}$$

- **Proof:**

- Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by last Theorem there are integers s and t with $b = a + sm$ and $d = c + tm$.
- Therefore,
 - $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and
 - $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$.
- Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Example: Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows from Theorem that

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$$

$$77 = 7 \times 11 \equiv 2 \times 1 = 2 \pmod{5}$$

Arithmetic Modulo m

- operations $+_m$ and \cdot_m satisfy many of the same properties as ordinary addition and multiplication.
 - Closure: If a and b belong to \mathbf{Z}_m , then $a +_m b$ and $a \cdot_m b$ belong to \mathbf{Z}_m .
 - Associativity: If a , b , and c belong to \mathbf{Z}_m , then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
 - Commutativity: If a and b belong to \mathbf{Z}_m , then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
 - Identity elements: The elements 0 and 1 are identity elements for addition and multiplication modulo m , respectively.
 - If a belongs to \mathbf{Z}_m , then $a +_m 0 = a$ and $a \cdot_m 1 = a$.

Arithmetic Modulo m

- Additive inverses: If $a \neq 0$ belongs to \mathbf{Z}_m , then $m - a$ is the additive inverse of a modulo m , and 0 is its own additive inverse.
 - $a +_m (m - a) = 0$ and $0 +_m 0 = 0$
- Distributivity: If a , b , and c belong to \mathbf{Z}_m , then
 - $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and
 - $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.
- Multiplicative inverses have not been included since they **do not always exist**. multiplicative inverse of a real number x is a real number y such that $xy = 1$.
- For example, there is no multiplicative inverse of 2 modulo 6.
- Use the definition of addition and multiplication in \mathbf{Z}_m **to find** $7 +_{11} 9$ **and** $7 \square_{11} 9$

Solution: Using the definition of addition modulo 11, we find that

- $7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5$, and
- $7 \square_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8$.
- Hence $7 +_{11} 9 = 5$ and $7 \square_{11} 9 = 8$.

Primes

Definition: A positive integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p . A positive integer that is greater than 1 and is not prime is called *composite*.

Example: The integer 7 is prime because its only positive factors are 1 and 7, but 9 is composite because it is divisible by 3.

Relative Prime Numbers: Two numbers are relatively prime, If GCD of two numbers is 1

The Fundamental Theorem of Arithmetic

Theorem: Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Examples:

Greatest Common Divisor

Definition: Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and also $d \mid b$ is called the greatest common divisor of a and b . The greatest common divisor of a and b is denoted by $\gcd(a,b)$.

One can find greatest common divisors of small numbers by inspection.

Example: What is the greatest common divisor of 24 and 36? **Solution:** $\gcd(24,36) = 12$

Example: What is the greatest common divisor of 17 and 22? **Solution:** $\gcd(17,22) = 1$

Greatest Common Divisor

Definition: The integers a and b are *relatively prime* if their greatest common divisor is 1.

Example: 17 and 22

Definition: 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: Determine whether the integers 10, 17 and 21 are pairwise relatively prime.

Solution: Because $\gcd(10,17) = 1$, $\gcd(10,21) = 1$, and $\gcd(17,21) = 1$, 10, 17, and 21 are pairwise relatively prime.

Example: Determine whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution: Because $\gcd(10,24) = 2$.

10, 19, and 24 are not pairwise relatively prime.

Finding the Greatest Common Divisor Using Prime Factorizations

- Suppose the prime factorizations of a and b are:

The image cannot be displayed. Your computer may not have enough memory to open the image or the image may have been corrupted. Reload your computer, and then open this page. If it's not a corrupted file, then it's likely that the file is too large. Try opening the image in a smaller window.

The image cannot be displayed. Your computer may not have enough memory to open the image or the image may have been corrupted. Reload your computer, and then open this page. If it's not a corrupted file, then it's likely that the file is too large. Try opening the image in a smaller window.

where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both. Then:

The image cannot be displayed. Your computer may not have enough memory to open the image or the image may have been corrupted. Reload your computer, and then open this page. If it's not a corrupted file, then it's likely that the file is too large. Try opening the image in a smaller window.

- This formula is valid since the integer on the right (of the equals sign) divides both a and b . No larger integer can divide both a and b .

Example: $120 = 2^3 \cdot 3 \cdot 5$ $500 = 2^2 \cdot 5^3$

$$\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20$$

- Finding the gcd of two positive integers using their prime factorizations is not efficient because there is **no efficient algorithm for finding the prime factorization of a positive integer**.

Least Common Multiple

Definition: The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b . It is denoted by $\text{lcm}(a,b)$.

- The least common multiple can also be computed from the prime factorizations.

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

This number is divided by both a and b and no smaller number is divided by a and b .

Example: $\text{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)} = 2^4 3^5 7^2$

- The greatest common divisor and the least common multiple of two integers are related by:

Theorem 5: Let a and b be positive integers. Then

$$ab = \gcd(a,b) \cdot \text{lcm}(a,b)$$

Euclidean Algorithm

- The Euclidean algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that, if $a > b$ and r is the remainder when a is divided by b , then $\gcd(a,b)$ is equal to $\gcd(b,r)$.

Example: Find $\gcd(91, 287)$:

- $287 = 91 \cdot 3 + 14$ Divide 287 by 91
- $91 = 14 \cdot 6 + 7$ Divide 91 by 14
- $14 = 7 \cdot 2 + 0$ Divide 14 by 7

$$\gcd(287, 91) = \gcd(91, 14) = \underbrace{\gcd(14, 7)}_{\text{Stopping condition}} = 7$$

Euclidean Algorithm

- The Euclidean algorithm expressed in pseudocode is:

```
procedure gcd( $a, b$ : positive integers)
```

```
 $x := a$ 
```

```
 $y := b$ 
```

```
while  $y \neq 0$ 
```

```
     $r := x \text{ mod } y$ 
```

```
     $x := y$ 
```

```
     $y := r$ 
```

```
return  $x$  {gcd( $a, b$ ) is  $x$ }
```

Correctness of Euclidean Algorithm

Lemma 1: Let $a = bq + r$, where a, b, q , and r are integers. Then $\gcd(a,b) = \gcd(b,r)$.

Proof:

- Suppose that d divides both a & b . Then d also divides $a - bq = r$. Hence, any common divisor of a and b must also be any common divisor of b and r .
- Suppose that d divides both b & r . Then d also divides $bq + r = a$. Hence, any common divisor of a and b must also be a common divisor of b and r .
- Therefore, $\gcd(a,b) = \gcd(b,r)$.

Solve using Euclidean Algorithm

- $\gcd(2322, 654)$
- Let $a = 2322$, $b = 654$.
- $2322 = 654 \cdot 3 + 360$
- $654 = 360 \cdot 1 + 294$
- $360 = 294 \cdot 1 + 66$
- $294 = 66 \cdot 4 + 30$
- $66 = 30 \cdot 2 + 6$
- $30 = 6 \cdot 5$
- Therefore, $\gcd(2322, 654) = 6$.

$$\begin{aligned}\gcd(2322, 654) &= \gcd(654, 360) \\ \gcd(654, 360) &= \gcd(360, 294) \\ \gcd(360, 294) &= \gcd(294, 66) \\ \gcd(294, 66) &= \gcd(66, 30) \\ \gcd(66, 30) &= \gcd(30, 6) \\ \gcd(30, 6) &= 6\end{aligned}$$

gcds as Linear Combinations

Bézout's Theorem: If a and b are positive integers, then there exist integers s and t such that $\gcd(a,b) = sa + tb$.

Definition: If a and b are positive integers, then integers s and t such that $\gcd(a,b) = sa + tb$ are called *Bézout coefficients* of a and b . The equation $\gcd(a,b) = sa + tb$ is called *Bézout's identity*.

- By Bézout's Theorem, the gcd of integers a and b can be expressed in the form $sa + tb$ where s and t are integers. This is a *linear combination* with integer coefficients of a and b .
 - $\text{Gcd}(6,14) = (-2)\cdot 6 + 1\cdot 14$
 - It first uses the Euclidean algorithm to find the gcd and then works backwards to express the gcd as a linear combination of the original two integers.

Finding gcds as Linear Combinations

Example: Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198.

Solution: First use the Euclidean algorithm to show $\gcd(252, 198) = 18$

Finding gcds as Linear Combinations

Example: Express $\gcd(102, 38)$ as a linear combination of 102 and 38.

Solution: First use the Euclidean algorithm find gcd.

$$102 = 2 * 38 + 26$$

$$38 = 1 * 26 + 12$$

$$26 = 2 * 12 + 2$$

$$12 = 6 * 2 + 0, \text{ So } \gcd(102, 38) = 2$$

Work backwards to find the *Bézout coefficients*

$$2 = 26 - 2 * 12$$

$$= 26 - 2 * (38 - 1 * 26)$$

$$= 3 * 26 - 2 * 38$$

$$= 3 * (102 - 2 * 38) - 2 * 38$$

$$=$$

So, the *Bézout coefficients* are 3 and -8

Find gcd(93, 219) using bezout coefficient:

$$219 = 93 \times 2 + 33$$

$$93 = 33 \times 2 + 27$$

$$33 = 27 \times 1 + 6$$

$$27 = 6 \times 4 + 3$$

$$6 = 3 \times 2 + 0$$

Gcd(93, 219) = 3.

$$3 = 27 - 4 \times 6$$

$$= 27 - 4 \times (33 - 27 \times 1)$$

$$= -4 \times 33 + 5 \times 27$$

$$= -4 \times 33 + 5 \times (93 - 2 \times 33)$$

$$= 5 \times 93 - 14 \times 33$$

$$= 5 \times 93 - 14 \times (219 - 2 \times 93)$$

$$= -14 \times 219 + 33 \times 93$$

**Therefore a solution to $\text{gcd}(93, 219) = 219x + 93y$ is
 $x = -14$ and $y = 33$.**

Multiplicative Inverse

- Multiplicative inverse can be calculated for the numbers which are relatively prime.

$$x \bmod n$$

Then multiplicative inverse y can be as follows:

$$x \times y \bmod n = 1$$

By using brute force method or by trial and error method we can get the value of y

Ex. for $3 \bmod 20$

$$3 \times y \bmod 20 = 1 \quad \text{we can try for numbers like } 2, 3, 4, 5, 6, 7$$

$$\therefore y = 7$$

But this is not an efficient method.

Multiplicative Inverse

- Find an inverse of 3 modulo 7 by first finding Bézout coefficients of 3 and 7.
- *Solution:* Because $\gcd(3, 7) = 1$,
 \therefore inverse of 3 modulo 7 exists. by Euclidean algorithm $7 = 2 \cdot 3 + 1$.
 - From this equation we see that $-2 \cdot 3 + 1 \cdot 7 = 1$.
 - This shows that -2 and 1 are Bézout coefficients of 3 and 7. We see that -2 is an inverse of 3 modulo 7.
 - Note that every integer congruent to -2 modulo 7 is also an inverse of 3, such as 5, -9, 12, and so on.
 - **As we know we can't have negative value as mod value.**

What are the solutions of the linear congruence $3x \equiv 4 \pmod{7}$?

- we know that -2 is an inverse of 3 modulo 7 . Multiplying both sides of the congruence by -2 shows that
 - $-2 \cdot 3x \equiv -2 \cdot 4 \pmod{7}$.
 - Because $-6 \equiv 1 \pmod{7}$ and $-8 \equiv 6 \pmod{7}$, it follows that if x is a solution, then $x \equiv -8 \equiv 6 \pmod{7}$.
 - We need to determine whether every x with $x \equiv 6 \pmod{7}$ is a solution.
 - Assume that $x \equiv 6 \pmod{7}$. Then,
 - it follows that $3x \equiv 3 \cdot 6 = 18 \equiv 4 \pmod{7}$,
 - which shows that all such x satisfy the congruence. We conclude that the solutions to the congruence are the integers x such that $x \equiv 6 \pmod{7}$, namely, $6, 13, 20, \dots$ and $-1, -8, -15, \dots$.

Find an inverse of 101 modulo 4620.

- *Solution:* First, we use the Euclidean algorithm to show that $\gcd(101, 4620) = 1$.
 - Then we will reverse the steps to find Bézout coefficients a and b such that $101a + 4620b = 1$. It will then follow that a is an inverse of 101 modulo 4620. The steps used by the Euclidean algorithm to find $\gcd(101, 4620)$ are

$$4620 = 45 \cdot 101 + 75$$

$$101 = 1 \cdot 75 + 26$$

$$75 = 2 \cdot 26 + 23$$

$$26 = 1 \cdot 23 + 3$$

$$3 = 7 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1.$$

- Because the last nonzero remainder is 1, we know that $\gcd(101, 4620) = 1$. We can now find the Bézout coefficients for 101 and 4620 by working backwards through these steps, expressing $\gcd(101, 4620) = 1$

We obtain $1 = 3 - 1 \cdot 2$

$$= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$$

$$= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$$

$$= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = -9 \cdot 75 + 26 \cdot 26$$

$$= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75) = 26 \cdot 101 - 35 \cdot 75$$

$$= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101) = -35 \cdot 4620 + 1601 \cdot 101.$$

That $-35 \cdot 4620 + 1601 \cdot 101 = 1$ tells us that -35 and 1601 are Bézout coefficients of 4620 and 101 ,
and **1601 is an inverse of 101 modulo 4620**.

- Here we are calculating multiplicative inverse for 101.

Base conversions

- Find the octal expansion of $(12345)_{10}$.

● **Solution:** First, divide 12345 by 8 to obtain

$$12345 = 8 \cdot 1543 + 1.$$

Successively dividing quotients by 8 gives

$$1543 = 8 \cdot 192 + 7,$$

$$192 = 8 \cdot 24 + 0,$$

$$24 = 8 \cdot 3 + 0,$$

$$3 = 8 \cdot 0 + 3.$$

The successive remainders that we have found, 1, 7, 0, 0, and 3, are the digits from the right to the left of 12345 in base 8. Hence, $(12345)_{10} = (30071)_8$.

- Find the hexadecimal expansion of $(177130)_{10}$.

Solution: First divide 177130 by 16 to obtain $177130 = 16 \cdot 11070 + 10$.

Successively dividing quotients by 16 gives

$$11070 = 16 \cdot 691 + 14,$$

$$691 = 16 \cdot 43 + 3,$$

$$43 = 16 \cdot 2 + 11,$$

$$2 = 16 \cdot 0 + 2.$$

The successive remainders that we have found, 10, 14, 3, 11, 2, give us the digits from the right to the left of 177130 in the hexadecimal (base 16) expansion of $(177130)_{10}$. It follows that $(177130)_{10} = (2B3EA)_{16}$.

CHINESE REMAINDER THEOREM

The Chinese remainder theorem (CRT) is used to solve a set of congruent equations with one variable but different moduli, which are relatively prime, as shown below:

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

...

$$x \equiv a_k \pmod{m_k}$$

THE CHINESE REMAINDER THEOREM Let m_1, m_2, \dots, m_n be pairwise relatively prime positive integers greater than one and a_1, a_2, \dots, a_n arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1},$$

$$x \equiv a_2 \pmod{m_2},$$

.

.

.

$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

CHINESE REMAINDER THEOREM

- *Theorem: Let m_1, m_2, \dots, m_r be positive integers such that m_i and m_j are relatively prime for $i \neq j$. Let $M = m_1 m_2 \cdots m_r$ and let u_1, u_2, \dots, u_r be integers. Then there exists exactly one integer u with $0 \leq u < M$ and $u \equiv u_i \pmod{m_i}$ for all $1 \leq i \leq r$.*
- *To construct a simultaneous solution, first let $M_k = M/m_k$ for $k = 1, 2, \dots, n$.*
- *That is, M_k is the product of the moduli.*
- *Because m_i and m_k have no common factors greater than 1 when $i = k$, it follows that $\gcd(m_k, M_k) = 1$.*
- *Consequently, we know that there is an integer y_k , an inverse of M_k modulo m_k , such that $M_k y_k \equiv 1 \pmod{m_k}$.*

CHINESE REMAINDER THEOREM

To construct a simultaneous solution, form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n.$$

First, note that because $M_j \equiv 0 \pmod{m_k}$ whenever $j = k$, all terms except the k th term in this sum are congruent to 0 modulo m_k .

Because $M_k y_k \equiv 1 \pmod{m_k}$ we see that

$x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$, for $k = 1, 2, \dots, n$. We have shown that x is a simultaneous solution to the n congruences.

Example

The following is an example of a set of equations with different moduli:

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

The solution to this set of equations is given in the next section; for the moment, note that the answer to this set of equations is $x = 23$. This value satisfies all equations: $23 \equiv 2 \pmod{3}$, $23 \equiv 3 \pmod{5}$, and $23 \equiv 2 \pmod{7}$.

Solution To Chinese Remainder Theorem

1. Find $M = m_1 \times m_2 \times \dots \times m_k$. This is the common modulus.
2. Find $M_1 = M/m_1, M_2 = M/m_2, \dots, M_k = M/m_k$.
3. Find the multiplicative inverse of M_1, M_2, \dots, M_k using the corresponding moduli (m_1, m_2, \dots, m_k). Call the inverses $M_1^{-1}, M_2^{-1}, \dots, M_k^{-1}$.
4. The solution to the simultaneous equations is

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \dots + a_k \times M_k \times M_k^{-1}) \bmod M$$

Example

Find the solution to the simultaneous equations:

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

Solution

We follow the four steps.

1. $M = 3 \times 5 \times 7 = 105$

2. $M_1 = 105 / 3 = 35, M_2 = 105 / 5 = 21, M_3 = 105 / 7 = 15$

3. The inverses are $M_1^{-1} = 2, M_2^{-1} = 1, M_3^{-1} = 1$

4. $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \pmod{105} = 223 \pmod{105}$

Example

Find all integers x which leave a remainder of 1, 2, 3, and 4 when divided by 5, 7, 9, and 11 respectively.

Solution: We are asked to solve the system of congruences:

$$x \equiv 1 \pmod{5}, x \equiv 2 \pmod{7}, x \equiv 3 \pmod{9}, x \equiv 4 \pmod{11}.$$

We have $M = 5 \cdot 7 \cdot 9 \cdot 11 = 3465$ and

$$M_1 = M/5 = 693,$$

$$M_2 = M/7 = 495,$$

$$M_3 = M/9 = 385, \text{ and}$$

$$M_4 = M/11 = 315.$$

The inverses are $y_1 = 2$, $y_2 = 3$, $y_3 = 4$, and $y_4 = 8$.

$$\text{Hence } x = 1 \cdot 693 \cdot 2 + 2 \cdot 495 \cdot 3 + 3 \cdot 385 \cdot 4 + 4 \cdot 315 \cdot 8 = 19056.$$

$$\text{So } x = [19056] \pmod{3465} = [1731] \pmod{3465}.$$

Example

Find an integer that has a remainder of 3 when divided by 7 and 13, but is divisible by 12.

Solution

This is a CRT problem. We can form three equations and solve them to find the value of x.

$$x = 3 \bmod 7$$

$$x = 3 \bmod 13$$

$$x = 0 \bmod 12$$

If we follow the four steps, we find $x = 276$. We can check that $276 = 3 \bmod 7$, $276 = 3 \bmod 13$ and 276 is divisible by 12 (the quotient is 23 and the remainder is zero).

Reference Book

- Cryptography and Information security,
second edition, by V. K. Pachghare.

Counting

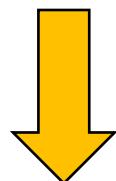
Basic Counting Principles

Product Rule:

Suppose a procedure consists of 2 tasks

n_1 ways to perform 1st task

n_2 ways to perform 2nd task



$n_1 \cdot n_2$ ways to perform procedure

Example: 2 employees 10 offices

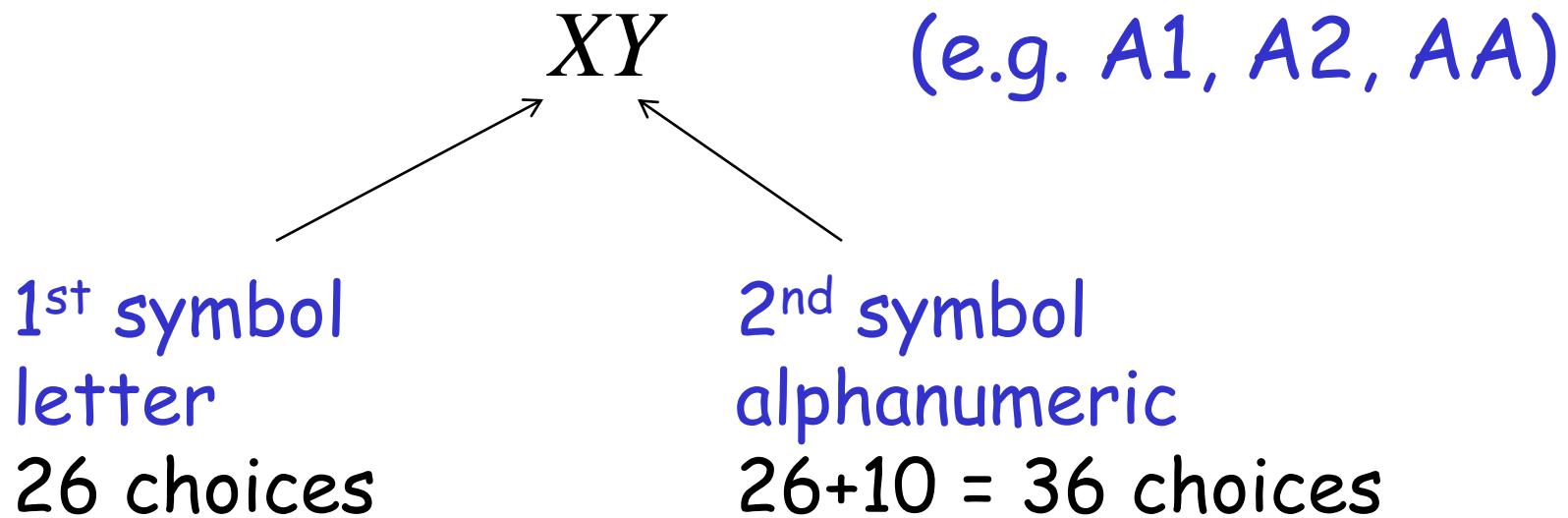
How many ways to assign employees to offices?

1st employee has 10 office choices

2nd employee has 9 office choices

Total office assignment ways: $10 \times 9 = 90$

Example: How many different variable names with 2 symbols?



Total variable name choices: $26 \times 36 = 936$

Generalized Product Rule:

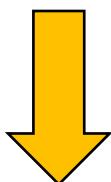
Suppose a procedure consists of k tasks

n_1 ways to perform 1st task

n_2 ways to perform 2nd task

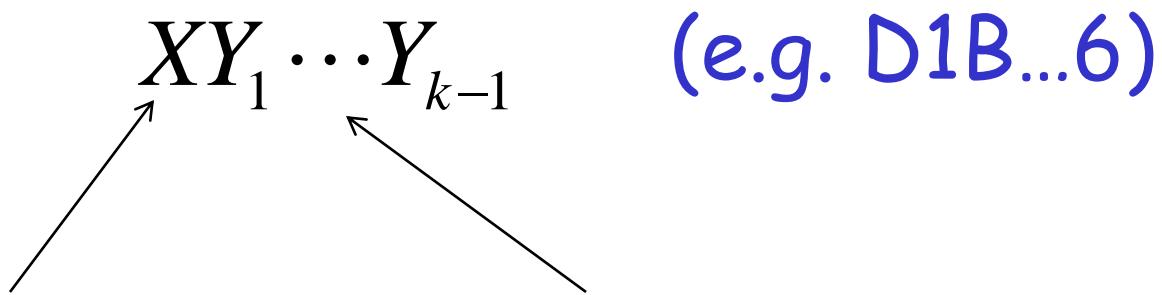
⋮

n_k ways to perform k th task



$n_1 n_2 \cdots n_k$ ways to perform procedure

Example: How many different variable names with exactly $k \geq 1$ symbols?



1st symbol
letter
26 choices

(e.g. D1B...6)

Remaining symbols
alphanumeric
36 choices for each

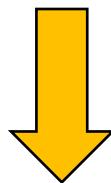
Total choices: $26 \cdot \underbrace{36 \cdots 36}_{k-1} = 26 \cdot (36)^{k-1}$

Sum Rule:

Suppose a procedure can be performed with either of 2 different methods

n_1 ways to perform 1st method

n_2 ways to perform 2nd method



$n_1 + n_2$ ways to perform procedure

Example: Number of variable names with
1 or 2 symbols

Variables with 1 symbol: 26

Variables with 2 symbols: 936

Total number of variables: $26+936=962$

Principle of Inclusion-Exclusion:

Suppose a procedure can be performed with either of 2 different methods

n_1 ways to perform 1st method

n_2 ways to perform 2nd method

c common ways in both methods



$n_1 + n_2 - c$ ways to perform procedure

Example:

Number of binary strings of length 8
that either start with 1 or end with 0

Strings that start with 1: $1x_1x_2 \cdots x_7$ 128 choices

Strings that end with 0: $y_1y_2 \cdots y_70$ 128 choices

Common strings: $1z_1 \cdots z_70$ 64 choices

Total strings: $128+128-64=192$

Selection (Ordered/ Unordered)

10 Boys and 8 girls
3 Boys and 3 Girls to be selected
How many ways?

Selecting 3 Boys
out of 10

(Order doesn't matter)

10 Boys

S S S NS NS NS NS NS NS

Selecting 3 Girls
out of 8

(Order doesn't matter)

8 Girls

S S S NS NS NS NS NS

$$\frac{10!}{3!7!} \times \frac{8!}{3!5!} = 6720$$

Counting Passwords

- Combining the sum and product rule allows us to solve more complex problems.

Example: Each user on a computer system has a password, which is six to eight characters long, where each character is an uppercase letter or a digit. Each password must contain at least one digit. How many possible passwords are there?

Counting Passwords

- Combining the sum and product rule allows us to solve more complex problems.

Example: Each user on a computer system has a password, which is six to eight characters long, where each character is an uppercase letter or a digit. Each password must contain at least one digit. How many possible passwords are there?

Solution: Let P be the total number of passwords, and let P_6 , P_7 , and P_8 be the passwords of length 6, 7, and 8.

- By the sum rule $P = P_6 + P_7 + P_8$.
- To find each of P_6 , P_7 , and P_8 , we find the number of passwords of the specified length composed of letters and digits and subtract the number composed only of letters. We find that:

$$P_6 = 36^6 - 26^6 = 2,176,782,336 - 308,915,776 = 1,867,866,560.$$

$$P_7 = 36^7 - 26^7 = \\ 78,364,164,096 - 8,031,810,176 = 70,332,353,920.$$

$$P_8 = 36^8 - 26^8 = \\ 2,821,109,907,456 - 208,827,064,576 = 2,612,282,842,880.$$

Consequently, $P = P_6 + P_7 + P_8 = 2,684,483,063,360$.

Circular Arrangements

Arrange 6 people
in a row

— — — — —

1st person → 6 ways

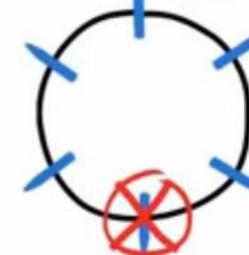
2nd person → 5 ways

⋮

⋮

6!

Arrange **6 people**
in a **circle**



1st person ~~6 ways~~

1st person → 1 way

2nd person → 5 ways

3rd person → 4 ways

⋮

5! ⋮ **1 × 5 !**

Pigeonhole Principle



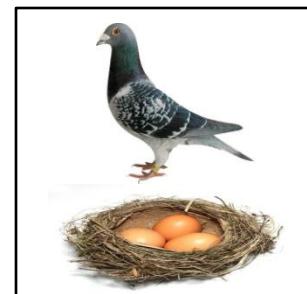
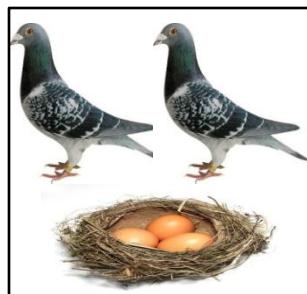
3 pigeons



2 pigeonholes

One pigeonhole contains 2 pigeons

3 pigeons



2 pigeonholes



• • • • •



$k+1$ pigeons



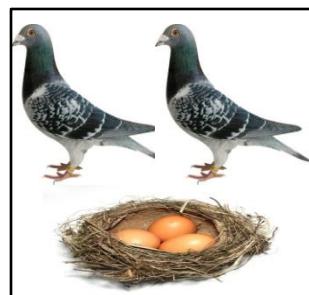
• • • • •



k pigeonholes

At least one pigeonhole contains 2 pigeons

$k+1$ pigeons



• • • • •



k pigeonholes

Pigeonhole Principle:

If $k+1$ objects are placed into k boxes,
then at least one box contains 2 objects

Examples:

- Among 367 people at least 2 have the same birthday (366 different birthdays)
- Among 27 English words at least 2 start with same letter (26 different letters)

Pigeonhole Principle

Example: How many students must be in a class to guarantee that at least two students receive the same score on the final exam, if the exam is graded on a scale from 0 to 100 points?

Solution: There are 101 possible scores on the final. The pigeonhole principle shows that among any 102 students there must be at least 2 students with the same score.

Pigeonhole Principle

Q. Assume there are n distinct pairs of shoes in a closet. Show that if you choose $n + 1$ single shoes at random from the closet, you are certain to have a pair.

Solution: The n distinct pairs constitute n pigeonholes. The $n + 1$ single shoes correspond to $n + 1$ pigeons.

Therefore, there must be at least one pigeonhole with two shoes and thus you will certainly have drawn at least one pair of shoes.

Pigeonhole Principle

Q. A student must take five classes from three areas of study. Numerous classes are offered in each discipline, but the student cannot take more than two classes in any given area. Using the pigeonhole principle, show that the student will take at least two classes in one area.

Solution: The three areas are the pigeonholes and the student must take five classes (pigeons). Hence, the student must take at least two classes in one area.

Generalized Pigeonhole Principle:

If N objects are placed into k boxes,
then at least one box contains $\left\lceil \frac{N}{k} \right\rceil$ objects

Proof:

If each box contains less than $\left\lceil \frac{N}{k} \right\rceil$ objects:

$$\#\text{objects} \leq k \left(\left\lceil \frac{N}{k} \right\rceil - 1 \right) < k \left(\left(\frac{N}{k} + 1 \right) - 1 \right) = N$$

contradiction

End of Proof

Example:

Among 100 people, at least $\left\lceil \frac{100}{12} \right\rceil = 9$ have birthday in same month

$N = 100$ people (objects)

$k = 12$ months (boxes)

Pigeonhole Principle

Q. Find the minimum number of students needed to guarantee that five of them belong to the same Class - 1st year, 2nd year, 3rd year, 4th year.

Solution: Here the $k = 4$ classes are the pigeonholes and $n + 1 = 5$ so $k = 4$. Thus among any $k \cdot n + 1 = 17$ students (pigeons), five of them belong to the same class.

Example:

How many students do we need to have so that at least six receive same grade (A,B,C,D,F)?

$N = ?$ students (objects)

$k = 5$ grades (boxes)

$$\left\lceil \frac{N}{k} \right\rceil \geq 6$$

at least six students receive same grade

Smallest integer N with $\left\lceil \frac{N}{k} \right\rceil \geq r$

is smallest integer with $\frac{N}{k} > r - 1$

$$\frac{N}{k} > r - 1 \quad \longrightarrow \quad N > k(r - 1) \quad \longrightarrow \quad N = k(r - 1) + 1$$

$$\left\lceil \frac{N}{k} \right\rceil \geq r \quad \longrightarrow \quad N = k(r-1) + 1$$

For our example:

$$k = 5 \quad \longrightarrow \quad N = 5(6-1) + 1 = 26 \text{ students}$$
$$r = 6$$

We need at least 26 students

An elegant example:

In any sequence of $n^2 + 1$ numbers
there is a sorted subsequence of length $n+1$
(ascending or descending)

$$n = 3$$

$$n + 1 = 4$$

Ascending
subsequence

$$n^2 + 1 = 10 \text{ numbers}$$

8, 11, 9, 1, 4, 6, 12, 10, 5, 7

Descending
subsequence

8, 11, 9, 1, 4, 6, 12, 10, 5, 7

Theorem:

In any sequence of $n^2 + 1$ numbers
there is a sorted subsequence of length $n+1$
(ascending or descending)

Proof: Sequence $a_1, a_2, a_3, \dots, a_{n^2+1}$

$$(x_i, y_i)$$

Length of longest
ascending subsequence
starting from a_i

Length of longest
descending subsequence
starting from a_i

For example: $(x_1, y_1) = (3,3)$

Longest ascending subsequence from $a_1 = 8$

8, 11, 9, 1, 4, 6, 12, 10, 5, 7

$$x_1 = 3$$

Longest descending subsequence from $a_1 = 8$

8, 11, 9, 1, 4, 6, 12, 10, 5, 7

$$y_1 = 3$$

For example: $(x_2, y_2) = (2, 4)$

Longest ascending subsequence from $a_2 = 11$

8, **11**, 9, 1, 4, 6, **12**, 10, 5, 7

$$x_2 = 2$$

Longest descending subsequence from $a_2 = 11$

8, **11**, **9**, 1, 4, **6**, 12, 10, **5**, 7

$$y_2 = 4$$

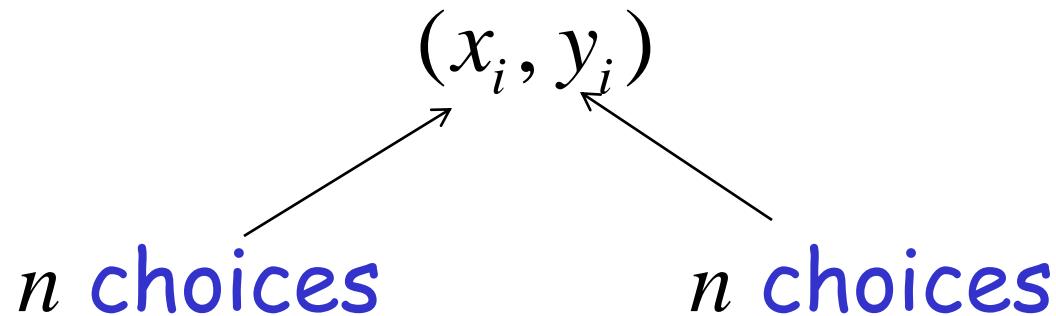
We want to prove that
there is a (x_i, y_i) with:

$$x_i \geq n + 1 \quad \text{or} \quad y_i \geq n + 1$$

Assume (for sake of contradiction) that
for every (x_i, y_i) :

$$1 \leq x_i \leq n \text{ and } 1 \leq y_i \leq n$$

Number of unique pairs of form (x_i, y_i)
with $1 \leq x_i \leq n$ and $1 \leq y_i \leq n$:

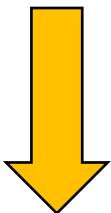


$$n \cdot n = n^2 \text{ unique pairs}$$

For example: $(1,1), (1,2), (2,1), (1,3), (3,1), \dots, (n,n)$

$n \cdot n = n^2$ unique pairs of form (x_i, y_i)

Since $a_1, a_2, a_3, \dots, a_{n^2+1}$ has $n^2 + 1$ elements
there are exactly $n^2 + 1$ pairs of form (x_i, y_i)



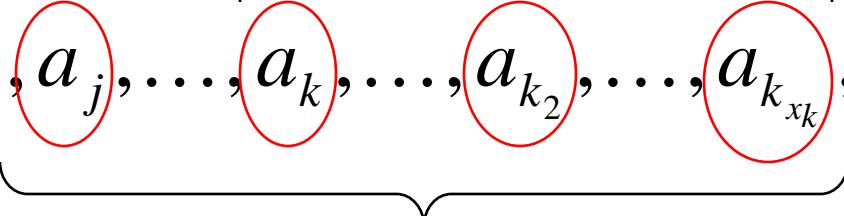
From pigeonhole principle, there are two equal pairs $(x_j, y_j) = (x_k, y_k)$, $j < k$

$$x_j = x_k \text{ and } y_j = y_k$$

Case $a_j \leq a_k$:

$$(x_j, y_j) = (x_k, y_k), \quad j < k \quad \longrightarrow \quad x_j = x_k$$

Ascending subsequence
with x_k elements

$$a_1, a_2, a_3, \dots, \underbrace{a_j, \dots, a_k, \dots, a_{k_2}, \dots, a_{k_{x_k}}, \dots, a_{n^2+1}}$$


Ascending subsequence
with $x_k + 1 = x_j + 1 > x_j$ elements

Contradiction, since longest ascending subsequence
from a_j has length x_j

Case $a_j > a_k$:

$$(x_j, y_j) = (x_k, y_k), \quad j < k \quad \longrightarrow \quad y_j = y_k$$

Descending subsequence
with y_k elements

$$a_1, a_2, a_3, \dots, \underbrace{a_j, \dots, a_k, \dots, a_{k_2}, \dots, a_{k_{y_k}}, \dots, a_{n^2+1}}_{\text{Descending subsequence with } y_k \text{ elements}}$$

Descending subsequence
with $y_k + 1 = y_j + 1 > y_j$ elements

Contradiction, since longest descending subsequence from a_j has length y_j

Therefore, it is not true the assumption
that for every (x_i, y_i) : $1 \leq x_i \leq n$ and $1 \leq y_i \leq n$

Therefore, there is a (x_i, y_i) with:

$$x_i \geq n + 1 \quad \text{or} \quad y_i \geq n + 1$$

End of Proof

Home work

- During a month with 30 days, a baseball team plays at least one game a day, but no more than 45 games. Show that there must be a period of some number of consecutive days during which the team must play exactly 14 games.

Permutations

Permutation: An ordered arrangement of objects

Example: Objects: a,b,c

Permutations: a,b,c a,c,b
 b,a,c b,c,a
 c,a,b c,b,a

r-permutation: An ordered arrangement of n objects

Example: Objects: a,b,c,d

2-permutations: a,b a,c a,d
b,a b,c b,d
c,a c,b c,d
d,a d,b d,c

How many ways to arrange 5 students in line?

1st position in line: 5 student choices

2nd position in line: 4 student choices

3rd position in line: 3 student choices

4th position in line: 2 student choices

5th position in line: 1 student choices

Total permutations: $5 \times 4 \times 3 \times 2 \times 1 = 120$

How many ways to arrange 3 students in line
out of a group of 5 students?

1st position in line: 5 student choices

2nd position in line: 4 student choices

3rd position in line: 3 student choices

Total 3-permutations: $5 \times 4 \times 3 = 60$

Given n objects the number of r -permutations is denoted

$$P(n, r)$$

Examples:

$$P(5,5) = 120$$

$$P(5,3) = 60$$

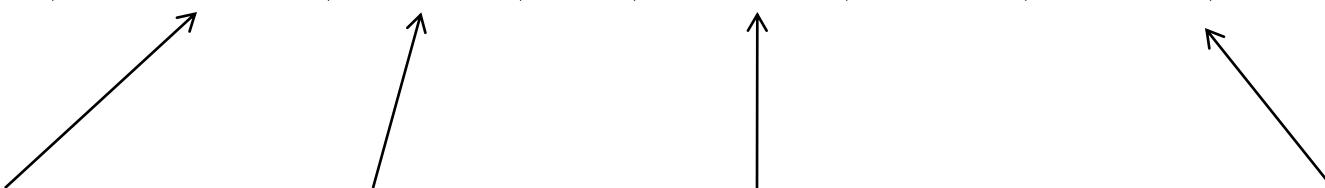
$$P(4,2) = 12$$

$$P(3,3) = 6$$

Theorem: $P(n, r) = \frac{n!}{(n - r)!}$ $0 \leq r \leq n$

Proof:

$$P(n, r) = n \cdot (n - 1) \cdot (n - 2) \cdots (n - (r - 1))$$



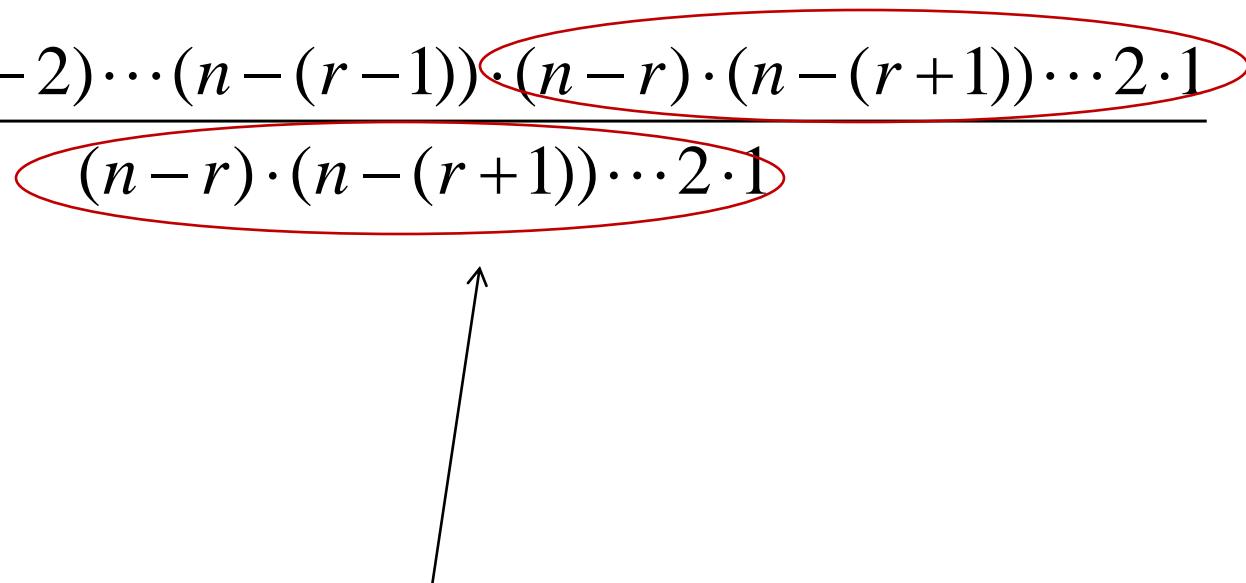
1st position
object
choices

2nd position
object
choices

3rd position
object
choices

r^{th} position
object
choices

$$P(n, r) = n \cdot (n-1) \cdot (n-2) \cdots (n-(r-1))$$

$$\begin{aligned} &= \frac{n \cdot (n-1) \cdot (n-2) \cdots (n-(r-1)) \cdot (n-r) \cdot (n-(r+1)) \cdots 2 \cdot 1}{(n-r) \cdot (n-(r+1)) \cdots 2 \cdot 1} \\ &= \frac{n!}{(n-r)!} \end{aligned}$$


Multiply and divide with same product

End of Proof

Example: How many different ways to order gold, silver, and bronze medalists out of 8 athletes?

$$P(8,3) = \frac{8!}{(8-3)!} = \frac{8!}{5!} = 8 \cdot 7 \cdot 6 = 336$$

Combinations

r-combination: An unordered arrangement of r objects

Example: Objects: a,b,c,d

2-combinations: a,b a,c a,d b,c b,d c,d

3-combinations: a,b,c a,b,d a,c,d b,c,d

Given n objects the number of
 r -combinations is denoted

$$C(n, r) \quad \text{or} \quad \binom{n}{r}$$

Also known as binomial coefficient

Examples: $C(4,2) = 6$

$$C(4,3) = 4$$

Combinations can be used to find permutations

3-combinations $C(4,3)$

a,b,c a,b,d a,c,d b,c,d

Objects: a,b,c,d

Combinations can be used to find permutations

3-permutations
 $P(3,3)$

3-combinations $C(4,3)$

a,b,c	a,b,d	a,c,d	b,c,d
a,c,b	a,d,b	a,d,c	b,d,c
b,a,c	b,a,d	c,a,d	c,b,d
b,c,a	b,d,a	c,d,a	c,d,b
c,a,b	d,a,b	d,a,c	d,b,c
c,b,a	d,b,a	d,c,a	d,c,b

Objects: a,b,c,d

Combinations can be used to find permutations

Total permutations: $P(4,3) = C(4,3) \cdot P(3,3)$

3-combinations $C(4,3)$

3-permutations
 $P(3,3)$

a,b,c	a,b,d	a,c,d	b,c,d
a,c,b	a,d,b	a,d,c	b,d,c
b,a,c	b,a,d	c,a,d	c,b,d
b,c,a	b,d,a	c,d,a	c,d,b
c,a,b	d,a,b	d,a,c	d,b,c
c,b,a	d,b,a	d,c,a	d,c,b

Objects: a,b,c,d

Theorem: $C(n, r) = \frac{n!}{r!(n - r)!}$ $0 \leq r \leq n$

Proof: $P(n, r) = C(n, r) \cdot P(r, r)$



$$C(n, r) = \frac{P(n, r)}{P(r, r)} = \frac{\frac{n!}{(n - r)!}}{\frac{r!}{(r - r)!}} = \frac{n!}{r!(n - r)!}$$

End of Proof

Example: Different ways to choose 5 cards out of 52 cards

$$C(52,5) = \frac{52!}{5!(47)!} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 26 \cdot 17 \cdot 10 \cdot 49 \cdot 12 = 2,598,960$$

Observation: $C(n, r) = C(n, n - r)$

$$C(n, r) = \frac{n!}{r!(n-r)!} = \frac{n!}{(n-(n-r))!(n-r)!} = C(n, n-r)$$

Example: $C(52, 5) = C(52, 47)$

Binomial Coefficients

$$C(n, r) = \binom{n}{r}$$

$$(x + y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y^1 + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n$$

$$(x + y)^n = \sum_{j=0}^n \binom{n}{j} x^{n-j} y^j$$

$$\begin{aligned}
 (x+y)^3 &= (x+y)(x+y)(x+y) \\
 &= xxx + xxy + xyx + xyy + yxx + yxy + yyx + yyy \\
 &= x^3 + 3x^2y + 3xy^2 + y^3
 \end{aligned}$$

$$(x+y)^3 = \binom{3}{0}x^3 + \binom{3}{1}x^2y + \binom{3}{2}xy^2 + \binom{3}{3}y^3$$

The diagram consists of three arrows originating from the text descriptions below and pointing towards the corresponding binomial coefficients in the equation above. The first arrow points to the term $\binom{3}{0}x^3$. The second arrow points to the term $\binom{3}{1}x^2y$. The third arrow points to the term $\binom{3}{3}y^3$.

Possible ways to obtain product of 3 terms of x and 0 terms of y

Possible ways to obtain product of 2 terms of x and 1 terms of y

Possible ways to obtain product of 0 terms of x and 3 terms of y

n times

$$(x+y)^n = \overbrace{(x+y)(x+y)(x+y) \cdots (x+y)}^{n \text{ times}}$$

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y^1 + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n$$

Possible ways to obtain product of n terms of x and 0 terms of y

Possible ways to obtain product of $n-1$ terms of x and 1 terms of y

Possible ways to obtain product of 0 terms of x and n terms of y

Binomial Coefficients

We know that a *binomial* is a polynomial that has two terms. In this section, you will study a formula that provides a quick method of raising a binomial to a power.

To begin, look at the expansion of $(x + y)^n$
for several values of n

$$(x + y)^0 = 1$$

$$(x + y)^1 = (x + y)$$

$$(x + y)^2 = x^2 + 2xy + y^2$$

$$(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$

$$(x + y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$$

Binomial Coefficients

1. The sum of the powers of each term is n . For instance, in the expansion of

$$(x + y)^5$$

the sum of the powers of each term is 5.

$$4 + 1 = 5 \quad 3 + 2 = 5$$

$$(x + y)^5 = x^5 + \overbrace{5x^4y^1}^{\text{ }} + \overbrace{10x^3y^2}^{\text{ }} + 10x^2y^3 + 5x^1y^4 + y^5$$

2. The coefficients increase and then decrease in a symmetric pattern.

The coefficients of a binomial expansion are called **binomial coefficients**.

Binomial Coefficients

- To find them, use the **Binomial Theorem**.

The Binomial Theorem

In the expansion of $(x + y)^n$

$$(x + y)^n = x^n + nx^{n-1}y + \cdots + {}_n C_r x^{n-r} y^r + \cdots + nxy^{n-1} + y^n$$

the coefficient of $x^{n-r} y^r$ is

$${}_n C_r = \frac{n!}{(n - r)!r!}.$$

The symbol

$$\binom{n}{r}$$

is often used in place of ${}_n C_r$ to denote binomial coefficients.

Example 1 – Finding Binomial Coefficients

Find each binomial coefficient.

a. $_8C_2$

b. $\binom{10}{3}$

c. $_7C_0$

a. $_8C_2 = \frac{8!}{6! \cdot 2!} = \frac{(8 \cdot 7) \cdot \cancel{6!}}{\cancel{6!} \cdot 2!} = \frac{8 \cdot 7}{2 \cdot 1} = 28$

b. $\binom{10}{3} = \frac{10!}{7! \cdot 3!} = \frac{(10 \cdot 9 \cdot 8) \cdot \cancel{7!}}{\cancel{7!} \cdot 3!} = \frac{10 \cdot 9 \cdot 8}{3 \cdot 2 \cdot 1} = 120$

c. $_7C_0 = \frac{\cancel{7!}}{\cancel{7!} \cdot 0!} = 1$

Example 3 – Expanding a Binomial

Write the expansion of the expression $(x + 1)^3$.

Solution:

The binomial coefficients are

$$3C_0 = 1, 3C_1 = 3, 3C_2 = 3, \text{ and } 3C_3 = 1.$$

Therefore, the expansion is as follows.

$$(x + 1)^3 = (1)x^3 + (3)x^2(1) + (3)x(1^2) + (1)(1^3)$$

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

Binomial Expansions

Sometimes you will need to find a specific term in a binomial expansion.

Instead of writing out the entire expansion, you can use the fact that, from the Binomial Theorem, the $(r + 1)$ th term is

$$nCr x^{n-r}y^r.$$

Example: What is the coefficient for x^3 in $(2x+4)^8$

Solution: The exponents for x^3 are: $(2x)^3 * 4^5$

The coefficient is "8 choose 5". We can use Pascal's Triangle, or calculate directly:

$$(n!/(k!(n-k)!))! = 8! / (5!(8-5)!) = 8! / (5!3!) = (8 \times 7 \times 6) / (3 \times 2 \times 1) = 56$$

And we get: $56(2x)^3 4^5$

Which simplifies to $458752 x^3$

Pascal's Triangle

$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	1
$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	1
$\begin{pmatrix} 2 \\ 0 \end{pmatrix}$	1
$\begin{pmatrix} 3 \\ 0 \end{pmatrix}$	1
$\begin{pmatrix} 4 \\ 0 \end{pmatrix}$	1
$\begin{pmatrix} 5 \\ 0 \end{pmatrix}$	1
$\begin{pmatrix} 6 \\ 0 \end{pmatrix}$	1
$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	1
$\begin{pmatrix} 2 \\ 1 \end{pmatrix}$	2
$\begin{pmatrix} 3 \\ 2 \end{pmatrix}$	3
$\begin{pmatrix} 4 \\ 3 \end{pmatrix}$	4
$\begin{pmatrix} 5 \\ 4 \end{pmatrix}$	5
$\begin{pmatrix} 6 \\ 4 \end{pmatrix}$	6
$\begin{pmatrix} 2 \\ 2 \end{pmatrix}$	2
$\begin{pmatrix} 3 \\ 3 \end{pmatrix}$	3
$\begin{pmatrix} 4 \\ 4 \end{pmatrix}$	4
$\begin{pmatrix} 5 \\ 5 \end{pmatrix}$	5
$\begin{pmatrix} 6 \\ 5 \end{pmatrix}$	5
$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	1
$\begin{pmatrix} 1 \\ 2 \end{pmatrix}$	6
$\begin{pmatrix} 2 \\ 3 \end{pmatrix}$	15
$\begin{pmatrix} 3 \\ 4 \end{pmatrix}$	20
$\begin{pmatrix} 4 \\ 5 \end{pmatrix}$	15
$\begin{pmatrix} 5 \\ 6 \end{pmatrix}$	6
$\begin{pmatrix} 6 \\ 6 \end{pmatrix}$	1

$$\begin{pmatrix} 6 \\ 4 \end{pmatrix} = \begin{pmatrix} 5 \\ 3 \end{pmatrix} + \begin{pmatrix} 5 \\ 4 \end{pmatrix}$$

$$15 = 10 + 5$$

Pascal's Triangle

The first and last number in each row of Pascal's Triangle is 1. Every other number in each row is formed by adding the two numbers immediately above the number. Pascal noticed that the numbers in this triangle are precisely the same numbers as the coefficients of binomial expansions, as follows.

$$(x + y)^0 = 1$$

0th row

$$(x + y)^1 = 1x + 1y$$

1st row

$$(x + y)^2 = 1x^2 + 2xy + 1y^2$$

2nd row

$$(x + y)^3 = 1x^3 + 3x^2y + 3xy^2 + 1y^3$$

3rd row

$$(x + y)^4 = 1x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + 1y^4 \quad :$$

$$(x + y)^5 = 1x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + 1y^5$$

$$(x + y)^6 = 1x^6 + 6x^5y + 15x^4y^2 + 20x^3y^3 + 15x^2y^4 + 6xy^5 + 1y^6$$

$$(x + y)^7 = 1x^7 + 7x^6y + 21x^5y^2 + 35x^4y^3 + 35x^3y^4 + 21x^2y^5 + 7xy^6 + 1y^7$$

Pascal's Triangle

The top row of Pascal's Triangle is called the *zeroth row* because it corresponds to the binomial expansion

$$(x + y)^0 = 1.$$

Similarly, the next row is called the *first row* because it corresponds to the binomial expansion

$$(x + y)^1 = 1(x) + 1(y).$$

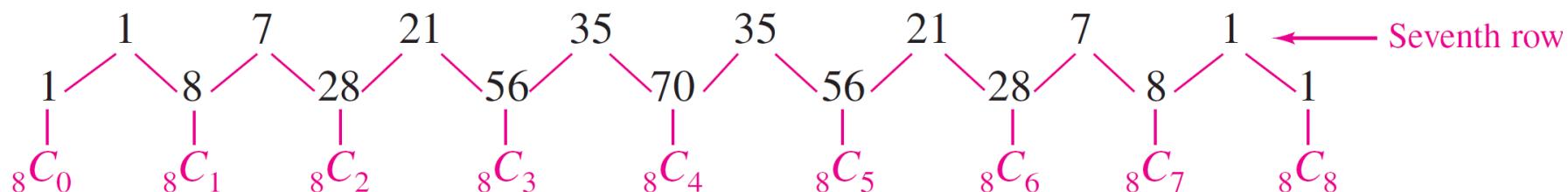
In general, the *n th row* of Pascal's Triangle gives the coefficients of $(x + y)^n$.

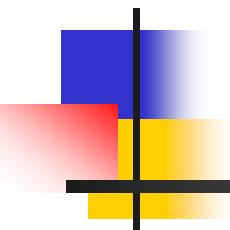
Example 8 – Using Pascal’s Triangle

Use the seventh row of Pascal’s Triangle to find the binomial coefficients.

$$8C_0 \ 8C_1 \ 8C_2 \ 8C_3 \ 8C_4 \ 8C_5 \ 8C_6 \ 8C_7 \ 8C_8$$

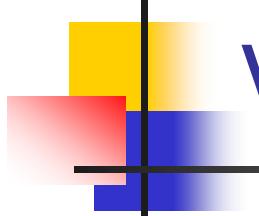
Solution:





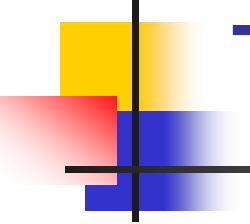
Graph Theory

Chapter 8



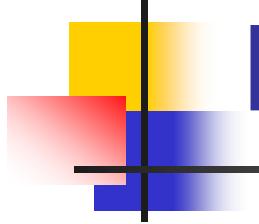
Varying Applications (examples)

- Computer networks
- Distinguish between two chemical compounds with the same molecular formula but different structures
- Solve shortest path problems between cities
- Scheduling exams and assign channels to television stations



Topics Covered

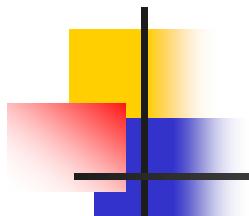
- Definitions
- Types
- Terminology
- Representation
- Sub-graphs
- Connectivity
- Hamilton and Euler definitions
- Shortest Path
- Planar Graphs
- Graph Coloring



Definitions - Graph

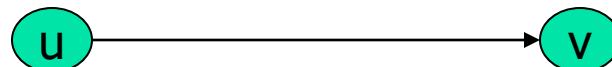
A generalization of the simple concept of a set of dots, links, edges or arcs.

Representation: Graph $G = (V, E)$ consists set of vertices denoted by V , or by $V(G)$ and set of edges E , or $E(G)$

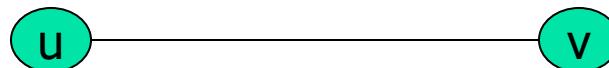


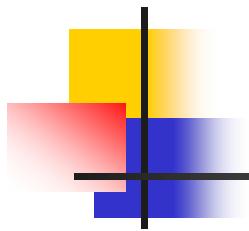
Definitions – Edge Type

Directed: Ordered pair of vertices. Represented as (u, v) directed from vertex u to v .



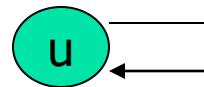
Undirected: Unordered pair of vertices. Represented as $\{u, v\}$. Disregards any sense of direction and treats both end vertices interchangeably.





Definitions – Edge Type

- **Loop:** A loop is an edge whose endpoints are equal i.e., an edge joining a vertex to it self is called a loop. Represented as $\{u, u\} = \{u\}$

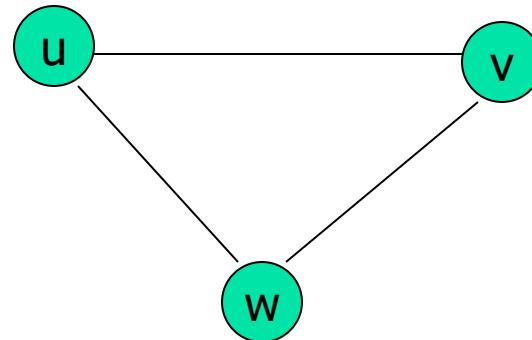


- **Multiple Edges:** Two or more edges joining the same pair of vertices.

Definitions – Graph Type

Simple (Undirected) Graph: consists of V , a nonempty set of vertices, and E , a set of unordered pairs of distinct elements of V called edges (undirected)

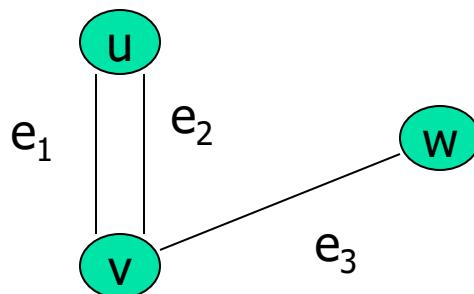
Representation Example: $G(V, E)$, $V = \{u, v, w\}$, $E = \{\{u, v\}, \{v, w\}, \{u, w\}\}$



Definitions – Graph Type

Multigraph: $G(V, E)$, consists of set of vertices V , set of Edges E and a function f from E to $\{\{u, v\} \mid u, v \in V, u \neq v\}$. The edges e_1 and e_2 are called multiple or parallel edges if $f(e_1) = f(e_2)$.

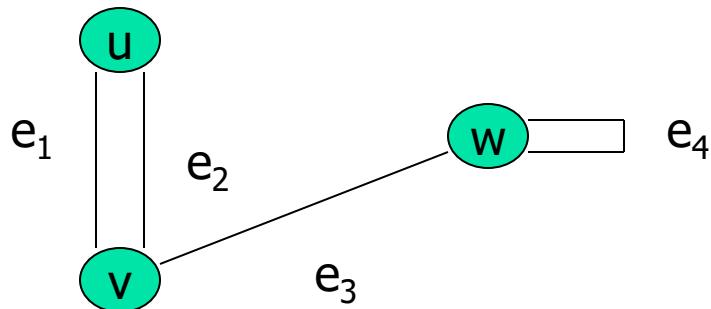
Representation Example: $V = \{u, v, w\}$, $E = \{e_1, e_2, e_3\}$



Definitions – Graph Type

Pseudograph: $G(V, E)$, consists of set of vertices V , set of Edges E and a function F from E to $\{\{u, v\} \mid u, v \in V\}$. Loops allowed in such a graph.

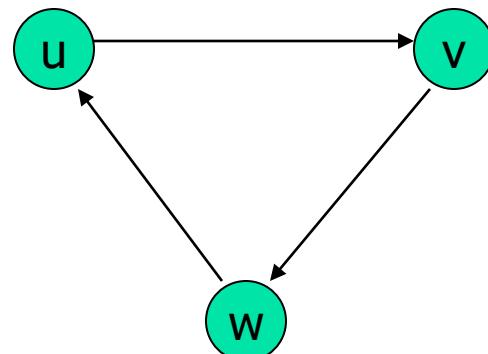
Representation Example: $V = \{u, v, w\}$, $E = \{e_1, e_2, e_3, e_4\}$



Definitions – Graph Type

Directed Graph: $G(V, E)$, set of vertices V , and set of Edges E , that are ordered pair of elements of V (directed edges)

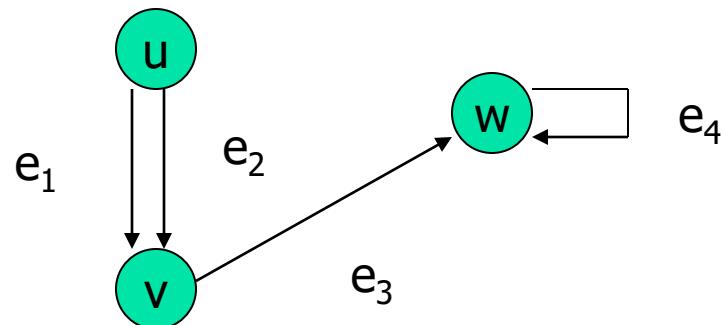
Representation Example: $G(V, E)$, $V = \{u, v, w\}$, $E = \{(u, v), (v, w), (w, u)\}$

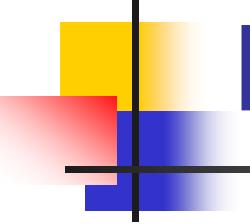


Definitions – Graph Type

Directed Multigraph: $G(V, E)$, consists of set of vertices V , set of Edges E and a function f from E to $\{\{u, v\} \mid u, v \in V\}$. The edges e_1 and e_2 are multiple edges if $f(e_1) = f(e_2)$

Representation Example: $V = \{u, v, w\}$, $E = \{e_1, e_2, e_3, e_4\}$





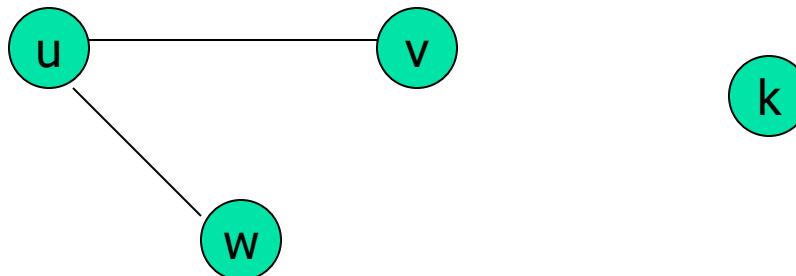
Definitions – Graph Type

Type	Edges	Multiple Edges Allowed ?	Loops Allowed ?
Simple Graph	undirected	No	No
Multigraph	undirected	Yes	No
Pseudograph	undirected	Yes	Yes
Directed Graph	directed	No	Yes
Directed Multigraph	directed	Yes	Yes

Terminology – Undirected graphs

- u and v are **adjacent** if $\{u, v\}$ is an edge, e is called **incident** with u and v . u and v are called **endpoints** of $\{u, v\}$
- **Degree of Vertex (deg (v)):** the number of edges incident on a vertex. A loop contributes twice to the degree (why?).
- **Pendant Vertex:** $\deg (v) = 1$
- **Isolated Vertex:** $\deg (k) = 0$

Representation Example: For $V = \{u, v, w\}$, $E = \{ \{u, w\}, \{u, v\} \}$, $\deg (u) = 2$, $\deg (v) = 1$, $\deg (w) = 1$, $\deg (k) = 0$, w and v are pendant , k is isolated

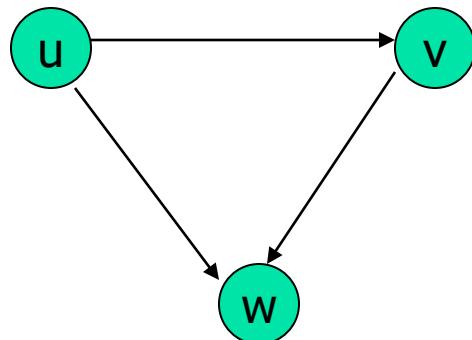


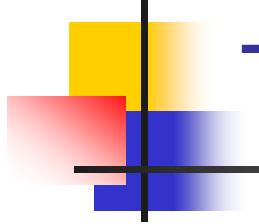
Terminology – Directed graphs

- For the edge (u, v) , u is **adjacent to** v OR v is **adjacent from** u , u – **Initial vertex**, v – **Terminal vertex**
- **In-degree ($\deg^- (u)$)**: number of edges for which u is terminal vertex
- **Out-degree ($\deg^+ (u)$)**: number of edges for which u is initial vertex

Note: A loop contributes 1 to both in-degree and out-degree (why?)

Representation Example: For $V = \{u, v, w\}$, $E = \{ (u, w), (v, w), (u, v) \}$, $\deg^-(u) = 0$, $\deg^+(u) = 2$, $\deg^-(v) = 1$, $\deg^+(v) = 1$, and $\deg^-(w) = 2$, $\deg^+(w) = 0$





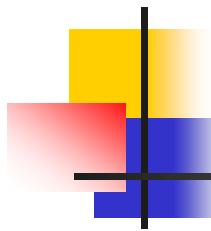
Theorems: Undirected Graphs

Theorem 1

The Handshaking theorem:

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

(why?) Every edge connects 2 vertices



Theorems: Undirected Graphs

Theorem 2:

An undirected graph has even number of vertices with odd degree

Proof V1 is the set of even degree vertices and V2 refers to odd degree vertices

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

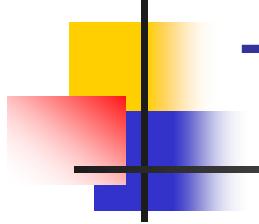
$\Rightarrow \deg(v)$ is even for $v \in V_1$,

\Rightarrow The first term in the right hand side of the last inequality is even.

\Rightarrow The sum of the last two terms on the right hand side of
the last inequality is even since sum is $2e$.

Hence second term is also even

$$\Rightarrow \text{second term } \sum_{v \in V_2} \deg(u) = \text{even}$$



Theorems: directed Graphs

- **Theorem 3:** $\sum \deg^+(u) = \sum \deg^-(u) = |E|$

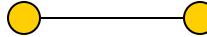
Simple graphs – special cases

- **Complete graph:** K_n , is the simple graph that contains exactly one edge between each pair of distinct vertices.

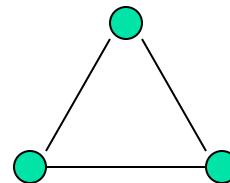
Representation Example: K_1, K_2, K_3, K_4



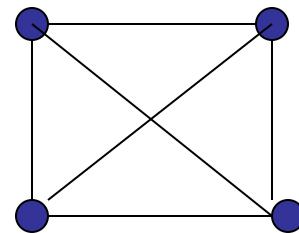
K_1



K_2



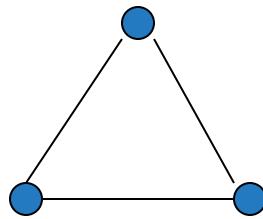
K_3



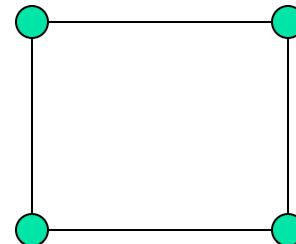
K_4

Simple graphs – special cases

- **Cycle:** C_n , $n \geq 3$ consists of n vertices $v_1, v_2, v_3 \dots v_n$ and edges $\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\} \dots \{v_{n-1}, v_n\}, \{v_n, v_1\}$
Representation Example: C_3, C_4



C_3

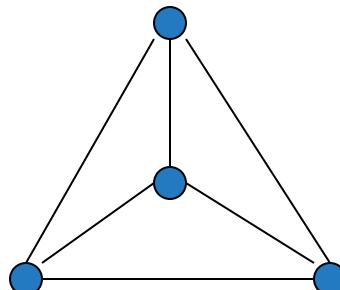


C_4

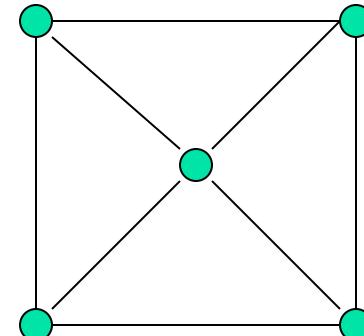
Simple graphs – special cases

- **Wheels:** W_n , obtained by adding additional vertex to C_n and connecting all vertices to this new vertex by new edges.

Representation Example: W_3 , W_4



W_3



W_4

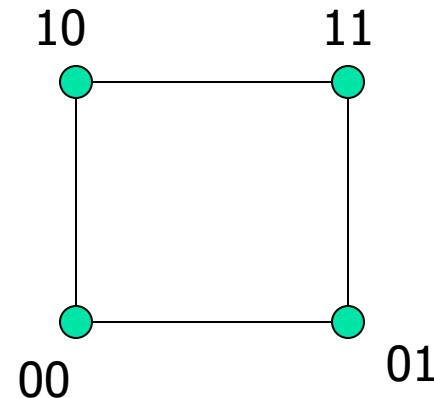
Simple graphs – special cases

- **N-cubes:** Q_n , vertices represented by $2n$ bit strings of length n . Two vertices are adjacent if and only if the bit strings that they represent differ by exactly one bit positions

Representation Example: Q_1 , Q_2



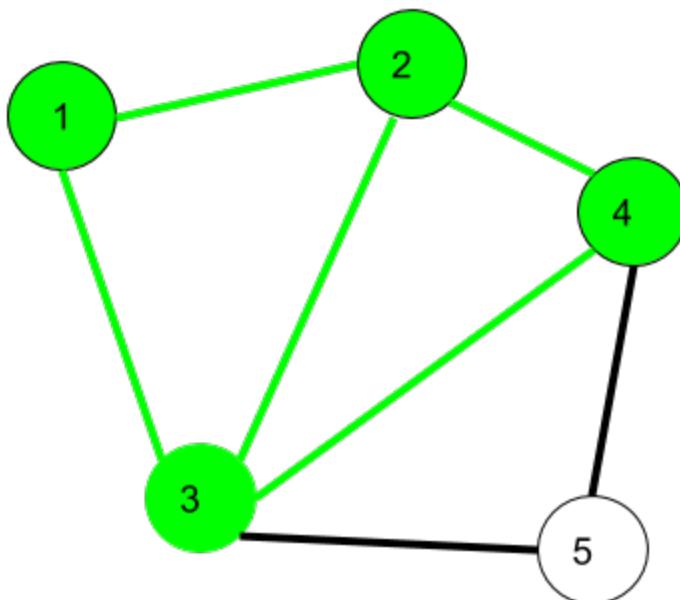
Q_1



Q_2

■ 1. Walk –

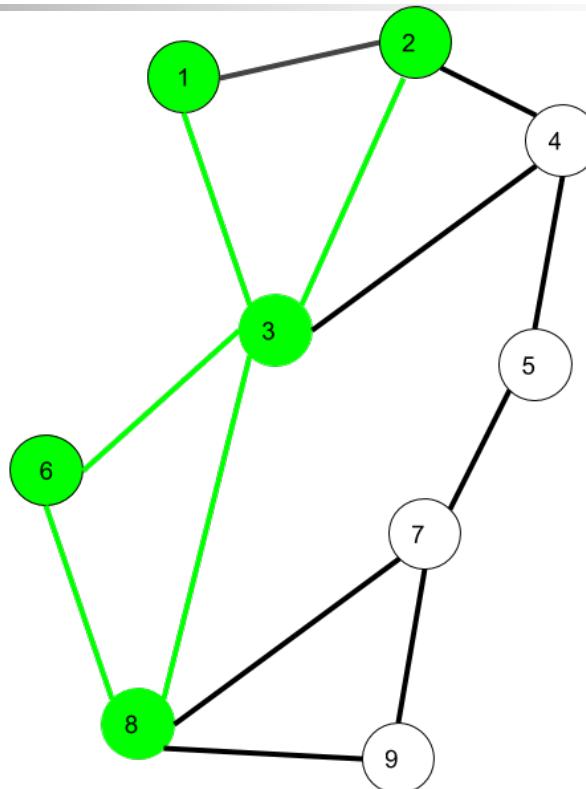
A walk is a sequence of vertices and edges of a graph i.e. if we traverse a graph then we get a walk.



- Here, $1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 2 \rightarrow 1 \rightarrow 3$ is a walk.

2. Trail –

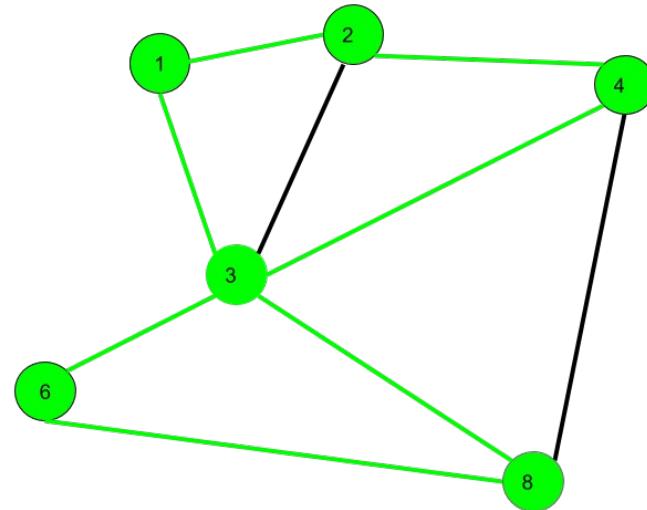
Trail is an open walk in which no edge is repeated.



- Here $1 \rightarrow 3 \rightarrow 8 \rightarrow 6 \rightarrow 3 \rightarrow 2$ is trail
Also $1 \rightarrow 3 \rightarrow 8 \rightarrow 6 \rightarrow 3 \rightarrow 2 \rightarrow 1$ will be a closed trail

Circuit –

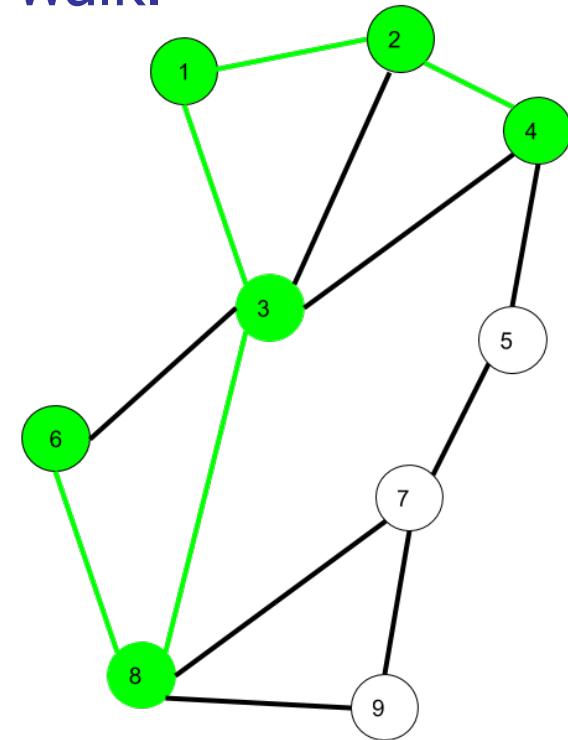
Traversing a graph such that not an edge is repeated but vertex can be repeated and it is closed also i.e. it is a closed trail.



- Here $1 \rightarrow 2 \rightarrow 4 \rightarrow 3 \rightarrow 6 \rightarrow 8 \rightarrow 3 \rightarrow 1$ is a circuit.

Path –

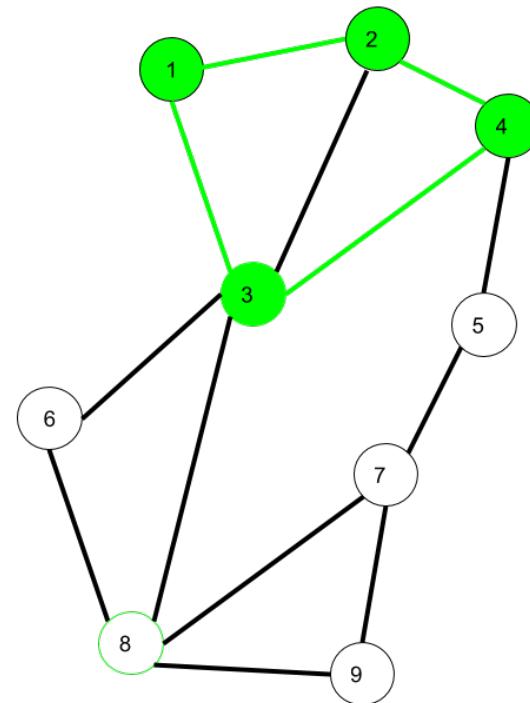
It is a trail in which neither vertices nor edges are repeated i.e. if we traverse a graph such that we do not repeat a vertex and nor we repeat an edge. As path is also a trail, thus it is also an open walk.



- Here $6 \rightarrow 8 \rightarrow 3 \rightarrow 1 \rightarrow 2 \rightarrow 4$ is a Path

Cycle –

Traversing a graph such that we do not repeat a vertex nor we repeat a edge but the starting and ending vertex must be same



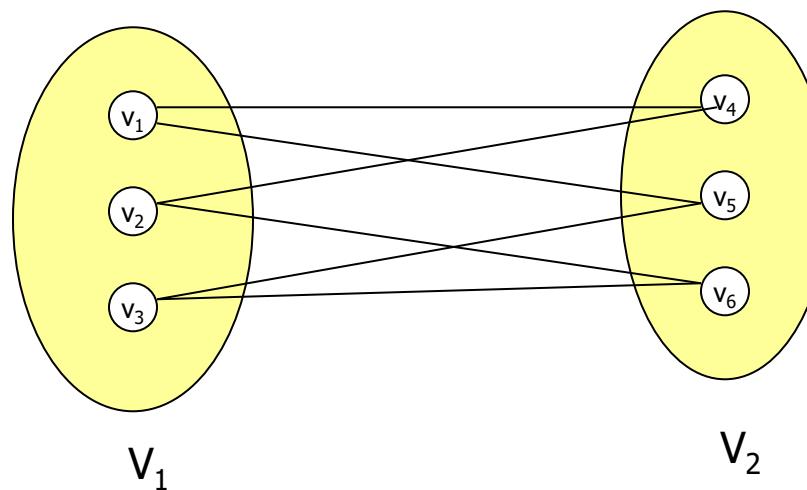
- Here $1 \rightarrow 2 \rightarrow 4 \rightarrow 3 \rightarrow 1$ is a cycle.

Bipartite graphs

- In a simple graph G , if 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 V_2 (so that no edge in G connects either two vertices in V_1 or two vertices in V_2)

Application example: Representing Relations

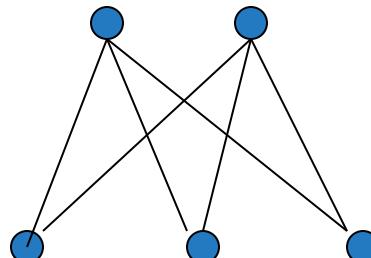
Representation example: $V_1 = \{v_1, v_2, v_3\}$ and $V_2 = \{v_4, v_5, v_6\}$,



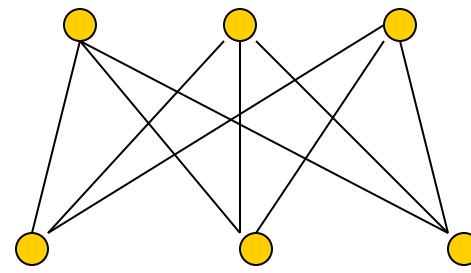
Complete Bipartite graphs

- $K_{m,n}$ is the graph that has its vertex set portioned into two subsets of m and n vertices, respectively. There is 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.

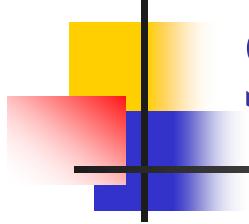
Representation example: $K_{2,3}$, $K_{3,3}$



$K_{2,3}$



$K_{3,3}$

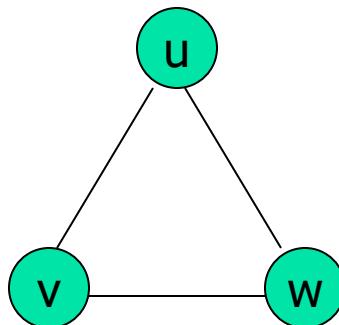


Subgraphs

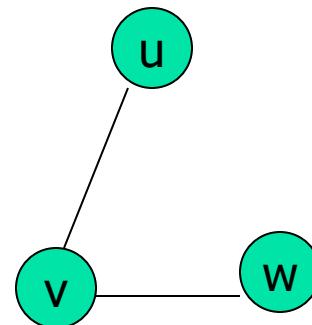
- A subgraph of a graph $G = (V, E)$ is a graph $H = (V', E')$ where V' is a subset of V and E' is a subset of E

Application example: solving sub-problems within a graph

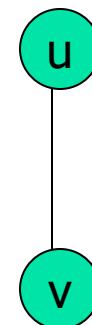
Representation example: $V = \{u, v, w\}$, $E = (\{u, v\}, \{v, w\}, \{w, u\})$, H_1 , H_2



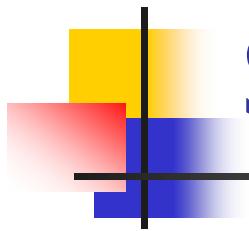
G



H_1



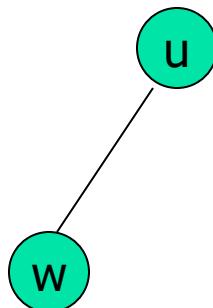
H_2



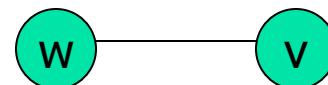
Subgraphs

- $G = G_1 \cup G_2$ wherein $E = E_1 \cup E_2$ and $V = V_1 \cup V_2$, G , G_1 and G_2 are simple graphs of G

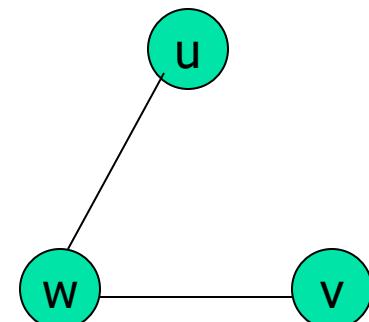
Representation example: $V_1 = \{u, w\}$, $E_1 = \{\{u, w\}\}$, $V_2 = \{w, v\}$,
 $E_2 = \{\{w, v\}\}$, $V = \{u, v, w\}$, $E = \{\{u, w\}, \{w, v\}\}$



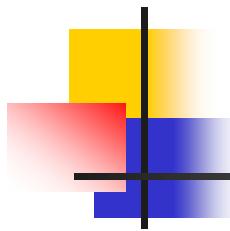
G_1



G_2

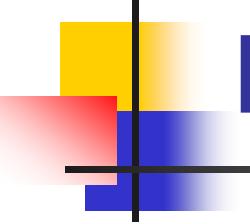


G



Representation

- **Incidence (Matrix):** Most useful when information about edges is more desirable than information about vertices.
- **Adjacency (Matrix/List):** Most useful when information about the vertices is more desirable than information about the edges. These two representations are also most popular since information about the vertices is often more desirable than edges in most applications



Representation- Incidence Matrix

- $G = (V, E)$ be an undirected graph. Suppose that $v_1, v_2, v_3, \dots, v_n$ 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 $M = [m_{ij}]$, where

$$m_{ij} = \begin{cases} 1 & \text{when edge } e_j \text{ is incident with } v_i \\ 0 & \text{otherwise} \end{cases}$$

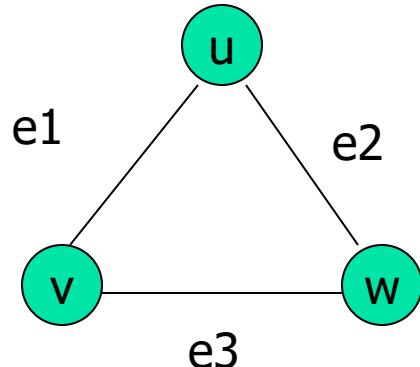
Can also be used to represent :

Multiple edges: by using columns with identical entries, since these edges are incident with the same pair of vertices

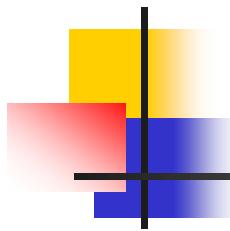
Loops: by using a column with exactly one entry equal to 1, corresponding to the vertex that is incident with the loop

Representation- Incidence Matrix

- Representation Example: $G = (V, E)$



	e_1	e_2	e_3
v	1	0	1
u	1	1	0
w	0	1	1



Representation- Adjacency Matrix

- There is an $N \times N$ matrix, where $|V| = N$, the Adjacent Matrix ($N \times N$) $A = [a_{ij}]$

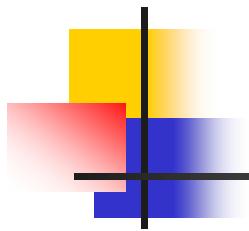
For undirected graph

$$a_{ij} = \begin{cases} 1 & \text{if } \{v_i, v_j\} \text{ is an edge of } G \\ 0 & \text{otherwise} \end{cases}$$

- **For directed graph**

$$a_{ij} = \begin{cases} 1 & \text{if } (v_i, v_j) \text{ is an edge of } G \\ 0 & \text{otherwise} \end{cases}$$

- This makes it easier to find subgraphs, and to reverse graphs if needed.

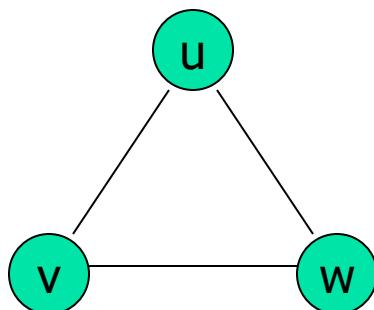


Representation- Adjacency Matrix

- Adjacency is chosen on the ordering of vertices. Hence, there are as many as $n!$ such matrices.
- The adjacency matrix of simple graphs are symmetric ($a_{ij} = a_{ji}$)
(why?)
- When there are relatively few edges in the graph the adjacency matrix is a **sparse matrix**
- Directed Multigraphs can be represented by using $a_{ij} = \text{number of edges from } v_i \text{ to } v_j$

Representation- Adjacency Matrix

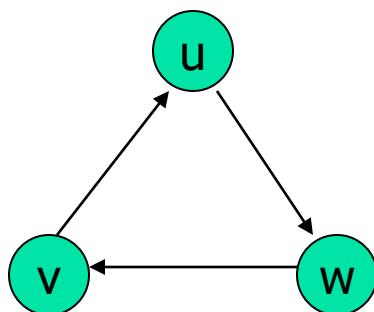
- Example: Undirected Graph $G(V, E)$



	v	u	w
v	0	1	1
u	1	0	1
w	1	1	0

Representation- Adjacency Matrix

- Example: directed Graph G (V, E)

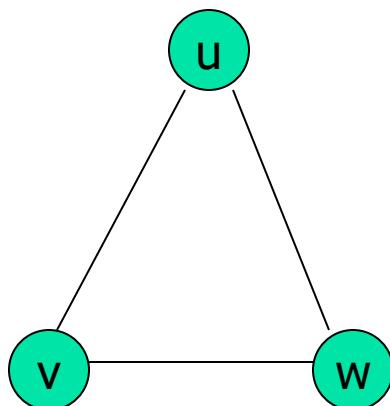


	v	u	w
v	0	1	0
u	0	0	1
w	1	0	0

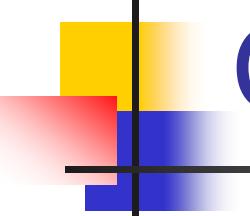
Representation- Adjacency List

Each node (vertex) has a list of which nodes (vertex) it is adjacent

Example: undirected graph $G(V, E)$



node	Adjacency List
u	v , w
v	w, u
w	u , v



Graph - Isomorphism

- $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic if:
- There is a one-to-one and onto function f from V_1 to V_2 with the property that
 - a and b are adjacent in G_1 if and only if $f(a)$ and $f(b)$ are adjacent in G_2 , for all a and b in V_1 .
- Function f is called isomorphism

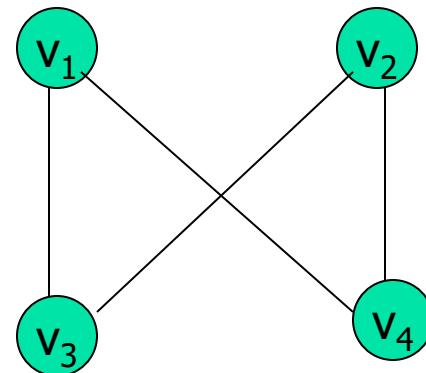
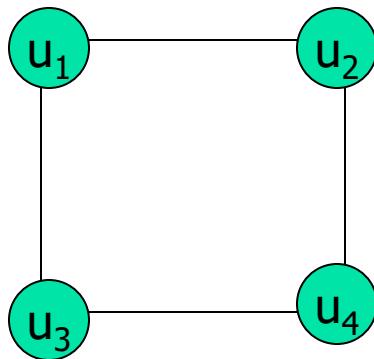
Application Example:

In chemistry, to find if two compounds have the same structure

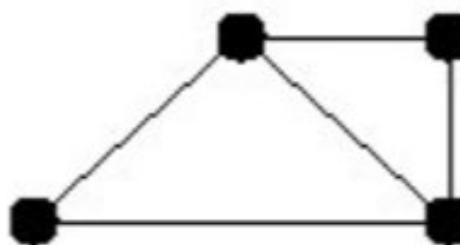
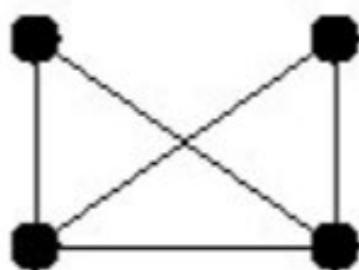
Graph - Isomorphism

Representation example: $G1 = (V1, E1)$, $G2 = (V2, E2)$

$f(u_1) = v_1, f(u_2) = v_4, f(u_3) = v_3, f(u_4) = v_2,$



Are the two graphs isomorphic?

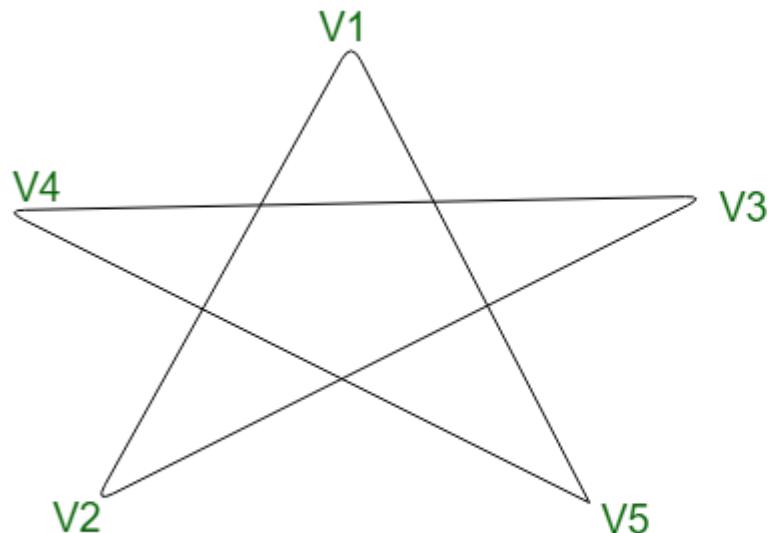


Solution

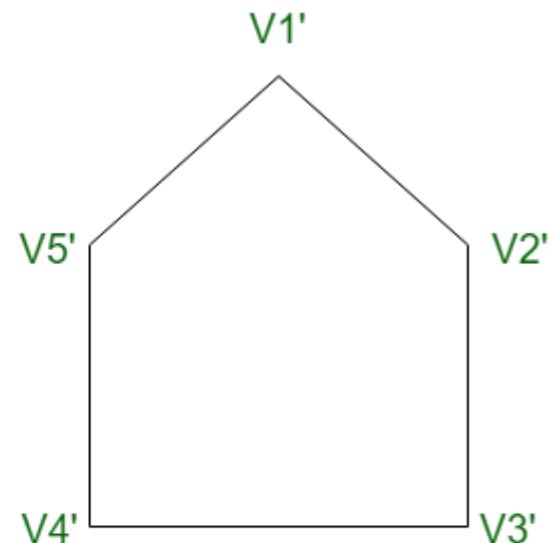
Yes, and corresponding vertices are labeled below.



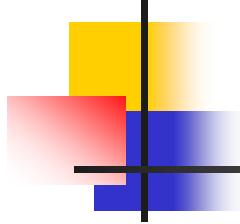
are isomorphic?



G



G'



Connectivity

- Basic Idea: In a Graph Reachability among vertices by traversing the edges

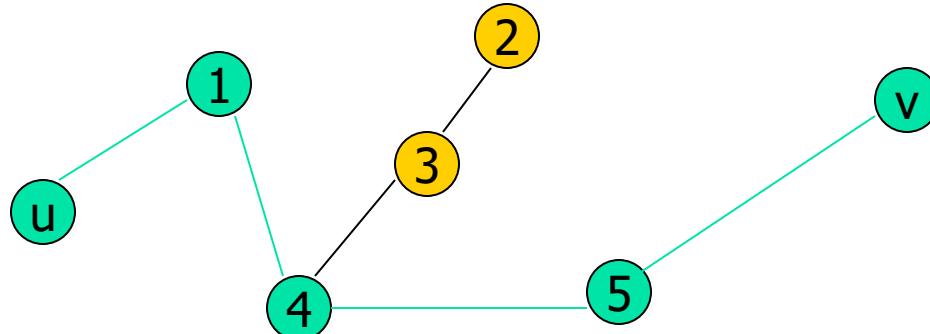
Application Example:

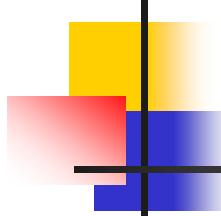
- In a city to city road-network, if one city can be reached from another city.
- Problems if determining whether a message can be sent between two computer using intermediate links
- Efficiently planning routes for data delivery in the Internet

Connectivity – Path

A **Path** is a sequence of edges that begins at a vertex of a graph and travels along edges of the graph, always connecting pairs of adjacent vertices.

Representation example: $G = (V, E)$, Path P represented, from u to v is $\{\{u, 1\}, \{1, 4\}, \{4, 5\}, \{5, v\}\}$





Connectivity – Path

Definition for Directed Graphs

A **Path** of length $n (> 0)$ from u to v in G is a sequence of n edges $e_1, e_2, e_3, \dots, e_n$ of G such that $f(e_1) = (x_0, x_1), f(e_2) = (x_1, x_2), \dots, f(e_n) = (x_{n-1}, x_n)$, where $x_0 = u$ and $x_n = v$. A path is said to pass through x_0, x_1, \dots, x_n or traverse $e_1, e_2, e_3, \dots, e_n$.

For Simple Graphs, sequence is x_0, x_1, \dots, x_n

In directed multigraphs when it is not necessary to distinguish between their edges, we can use sequence of vertices to represent the path

Circuit/Cycle: $u = v$, length of path > 0

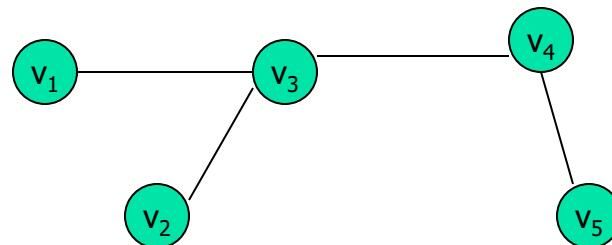
Simple Path: does not contain an edge more than once

Connectivity – Connectedness

Undirected Graph

An undirected graph is connected if there exists a simple path between every pair of vertices

Representation Example: $G(V, E)$ is connected since for $V = \{v_1, v_2, v_3, v_4, v_5\}$, there exists a path between $\{v_i, v_j\}$, $1 \leq i, j \leq 5$

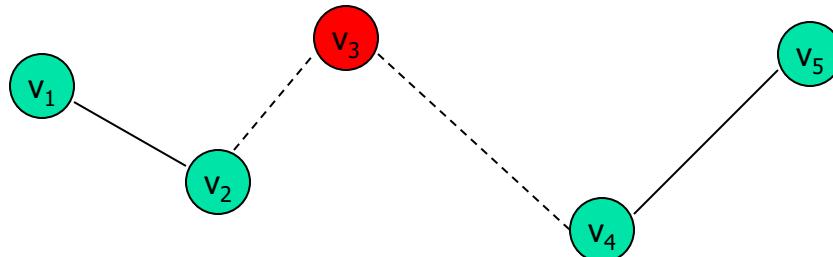


Connectivity – Connectedness

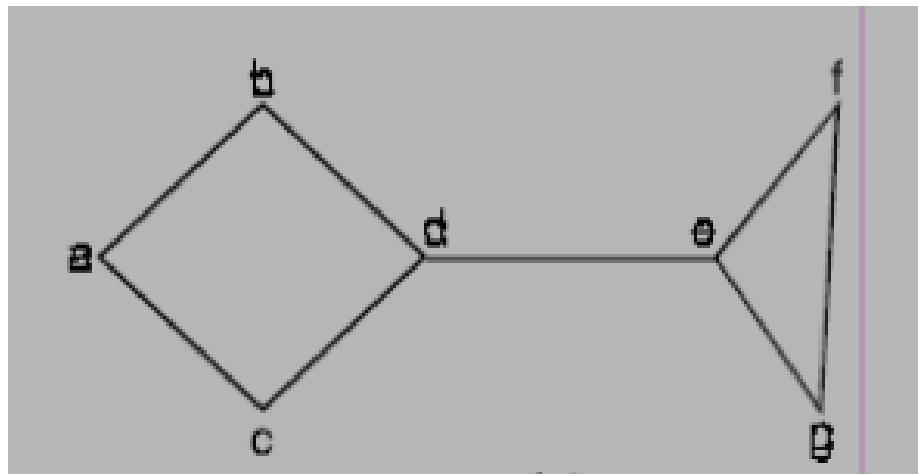
Undirected Graph

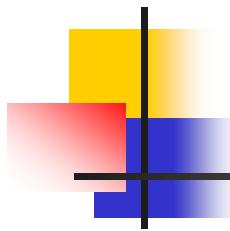
- **Articulation Point (Cut vertex):** removal of a vertex produces a subgraph with more connected components than in the original graph. The removal of a cut vertex from a connected graph produces a graph that is not connected
- **Cut Edge:** An edge whose removal produces a subgraph with more connected components than in the original graph.

Representation example: $G(V, E)$, v_3 is the articulation point or edge $\{v_2, v_3\}$, the number of connected components is 2 (> 1)



Find cut vertex and cut edge





Connectivity – Connectedness

Directed Graph

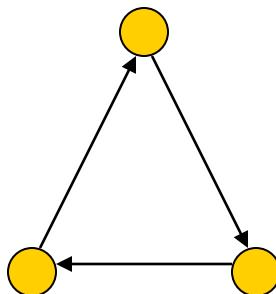
- A directed graph is **strongly connected** if there is a path from a to b and from b to a whenever a and b are vertices in the graph
- A directed graph is **weakly connected** if there is a (undirected) path between every two vertices in the underlying undirected path

A strongly connected Graph can be weakly connected but the vice-versa is not true (why?)

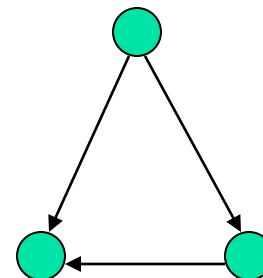
Connectivity – Connectedness

Directed Graph

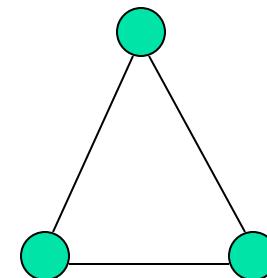
Representation example: G1 (Strong component), G2 (Weak Component), G3 is undirected graph representation of G2 or G1



G1



G2



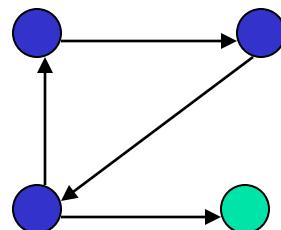
G3

Connectivity – Connectedness

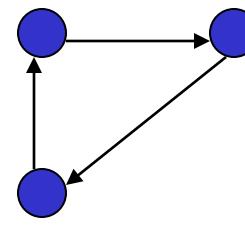
- **Directed Graph**

Strongly connected Components: subgraphs of a Graph G that are strongly connected

Representation example: G1 is the strongly connected component in G



G

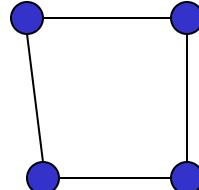


G1

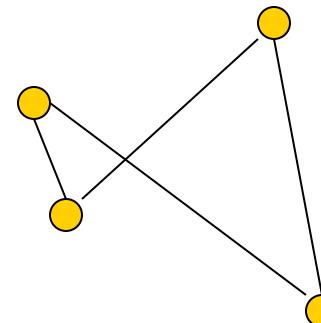
Isomorphism - revisited

A isomorphic invariant for simple graphs is the existence of a simple circuit of length k , k is an integer > 2 (why ?)

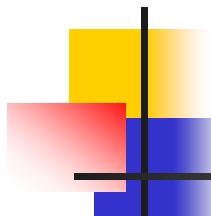
Representation example: G_1 and G_2 are isomorphic since we have the invariants, similarity in degree of nodes, number of edges, length of circuits



G_1



G_2



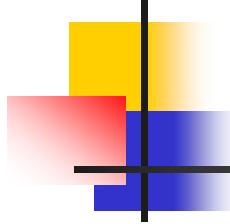
Counting Paths

- **Theorem:** Let G be a graph with adjacency matrix A with respect to the ordering v_1, v_2, \dots, v_n (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 $(i, j)^{\text{th}}$ entry of (adjacency matrix) A^r .

Proof: By Mathematical Induction.

Base Case: For the case $N = 1$, $a_{ij} = 1$ implies that there is a path of length 1. This is true since this corresponds to an edge between two vertices.

We assume that theorem is true for $N = r$ and prove the same for $N = r + 1$. Assume that the $(i, j)^{\text{th}}$ entry of A^r is the number of different paths of length r from v_i to v_j . By induction hypothesis, b_{ik} is the number of paths of length r from v_i to v_k .



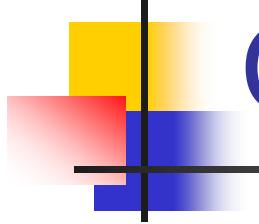
Counting Paths

Case $r + 1$: In $A^{r+1} = A^r \cdot A$,

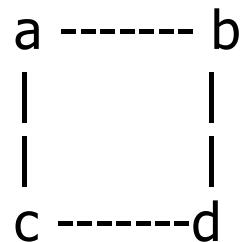
The $(i, j)^{\text{th}}$ entry in A^{r+1} , $b_{i1}a_{1j} + b_{i2}a_{2j} + \dots + b_{in}a_{nj}$
where b_{ik} is the $(i, j)^{\text{th}}$ entry of A^r .

By induction hypothesis, b_{ik} is the number of paths of length r from v_i to v_k .

The $(i, j)^{\text{th}}$ entry in A^{r+1} corresponds to the length between i and j and the length is $r+1$. This path is made up of length r from v_i to v_k and of length from v_k to v_j . By product rule for counting, the number of such paths is $b_{ik} * a_{kj}$. The result is $b_{i1}a_{1j} + b_{i2}a_{2j} + \dots + b_{in}a_{nj}$, the desired result.

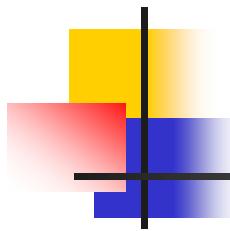


Counting Paths



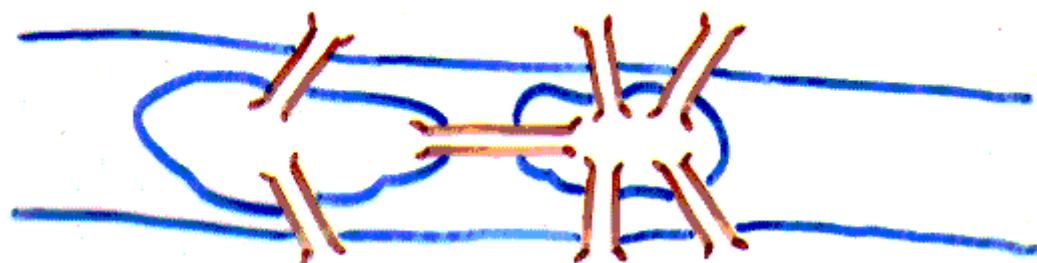
$$A = \begin{matrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{matrix} \quad A^4 = \begin{matrix} 8 & 0 & 0 & 8 \\ 0 & 8 & 8 & 0 \\ 0 & 8 & 8 & 0 \\ 8 & 0 & 0 & 8 \end{matrix}$$

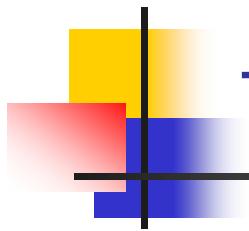
Number of paths of length 4 from a to d is (1,4) th entry of $A^4 = 8$.



The Seven Bridges of Königsberg, Germany

- The residents of Königsberg, Germany, wondered if it was possible to take a walking tour of the town that crossed each of the seven bridges over the Presel river exactly once. Is it possible to start at some node and take a walk that uses each edge exactly once, and ends at the starting node?

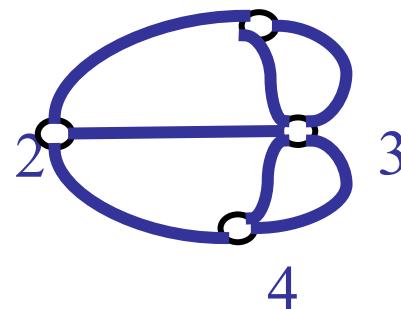




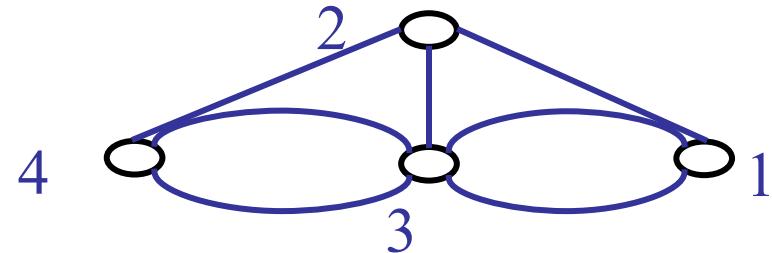
The Seven Bridges of Königsberg, Germany

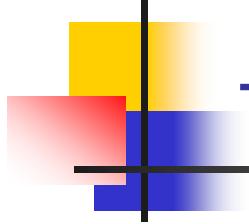
You can redraw the original picture as long as for every edge between nodes i and j in the original you put an edge between nodes i and j in the redrawn version (and you put no other edges in the redrawn version).

Original:



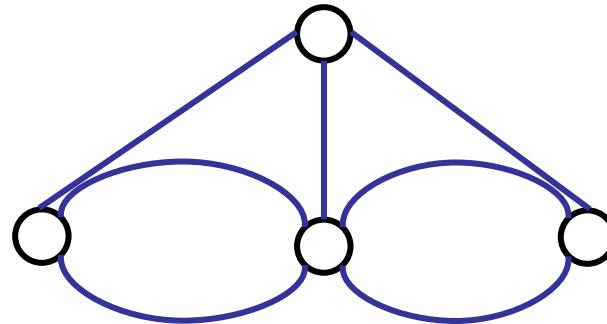
Redrawn:





The Seven Bridges of Königsberg, Germany

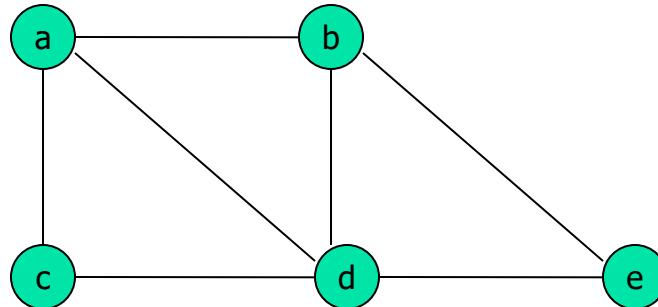
Euler:

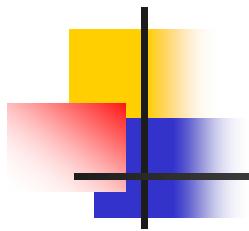


- Has no tour that uses each edge exactly once.
- (Even if we allow the walk to start and finish in different places.)
- Can you see why?

Euler - definitions

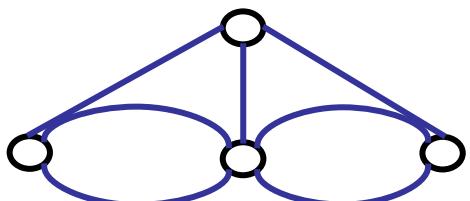
- An **Eulerian path** (**Eulerian trail**, **Euler walk**) in a graph is a path that uses each edge precisely once. If such a path exists, the graph is called **traversable**.
- An **Eulerian cycle** (**Eulerian circuit**, **Euler tour**) in a graph is a cycle that uses each edge precisely once. If such a cycle exists, the graph is called **Eulerian** (also **unicursal**).
- Representation example: G1 has Euler path a, c, d, e, b, d, a, b





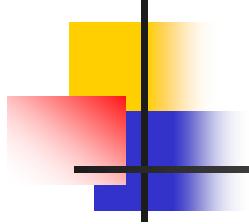
The problem in our language:

Show that



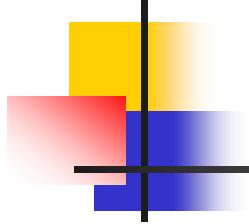
is not Eulerian.

In fact, it contains no Euler trail.



Euler - theorems

1. A connected graph G is Eulerian if and only if G is connected and has no vertices of odd degree
2. A connected graph G has an Euler trail from node a to some other node b if and only if G is connected and $a \neq b$ are the only two nodes of odd degree



Euler – theorems (\Rightarrow)

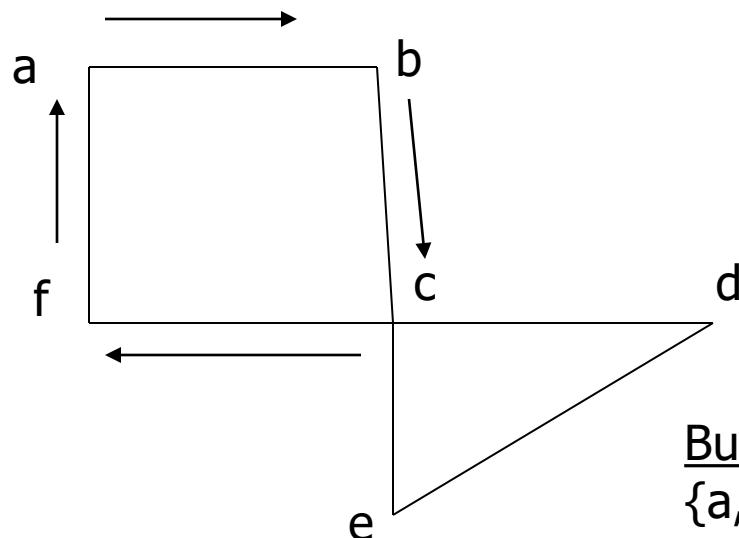
Assume G has an Euler trail T from node a to node b (a and b not necessarily distinct).

For every node besides a and b , T uses an edge to exit for each edge it uses to enter. Thus, the degree of the node is even.

1. If $a = b$, then a also has even degree. \rightarrow Euler circuit
2. If $a \neq b$, then a and b both have odd degree. \rightarrow Euler path

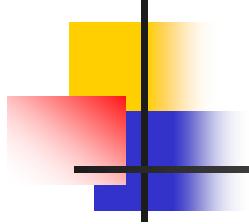
Euler - theorems

1. A connected graph G is Eulerian if and only if G is connected and has no vertices of odd degree



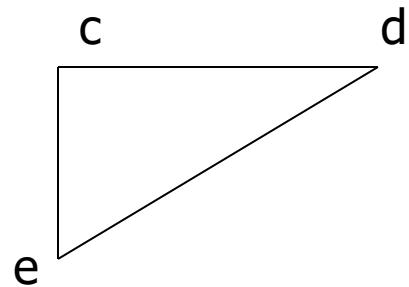
Building a simple path:
 $\{a,b\}, \{b,c\}, \{c,f\}, \{f,a\}$

Euler circuit constructed if all edges are used. True here?



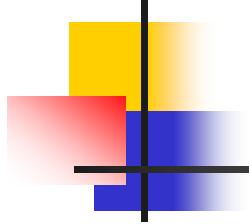
Euler - theorems

1. A connected graph G is Eulerian if and only if G is connected and has no vertices of odd degree



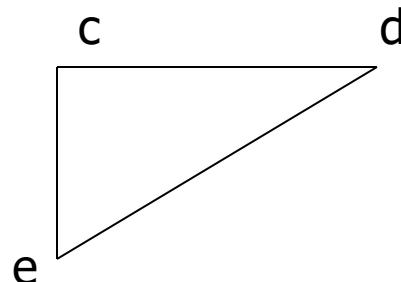
Delete the simple path:
 $\{a,b\}, \{b,c\}, \{c,f\}, \{f,a\}$

C is the common vertex for this sub-graph with its “parent”.



Euler - theorems

1. A connected graph G is Eulerian if and only if G is connected and has no vertices of odd degree



Constructed subgraph may not be connected.

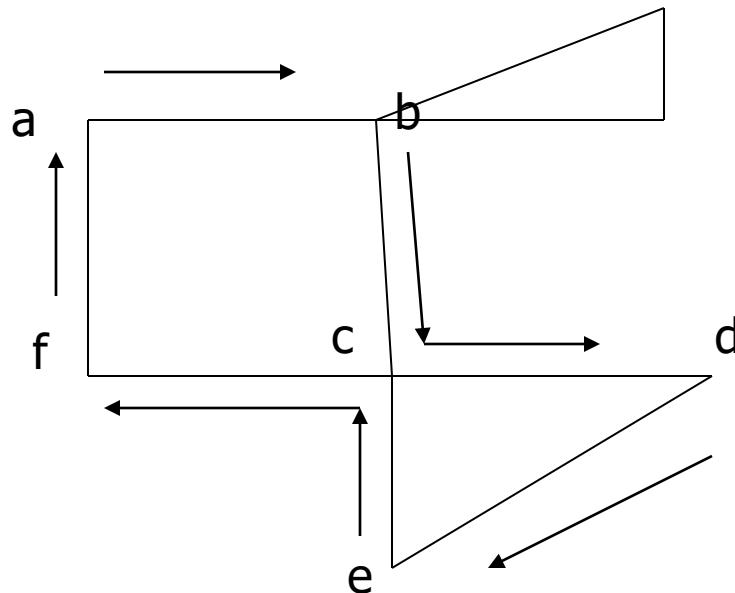
C is the common vertex for this sub-graph with its “parent”.

C has even degree.

Start at c and take a walk:
 $\{c,d\}, \{d,e\}, \{e,c\}$

Euler - theorems

1. A connected graph G is Eulerian if and only if G is connected and has no vertices of odd degree



"Splice" the circuits in the 2 graphs:

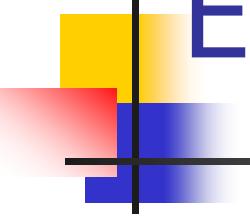
$\{a,b\}, \{b,c\}, \{c,f\}, \{f,a\}$

“+”

$\{c,d\}, \{d,e\}, \{e,c\}$

“=”

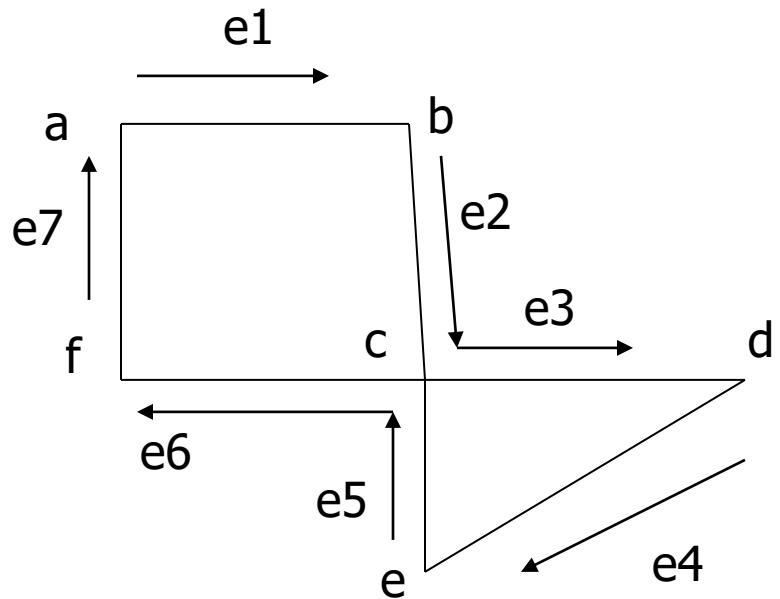
$\{a,b\}, \{b,c\}, \{c,d\}, \{d,e\}, \{e,c\}, \{c,f\}$
 $\{f,a\}$



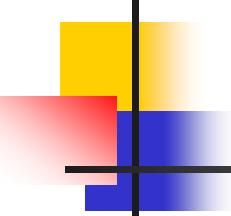
Euler Circuit

1. Circuit $C :=$ a circuit in G beginning at an arbitrary vertex v .
 1. Add edges successively to form a path that returns to this vertex.
2. $H := G -$ above circuit C
3. While H has edges
 1. Sub-circuit $sc :=$ a circuit that begins at a vertex in H that is also in C (e.g., vertex "c")
 2. $H := H - sc$ (- all isolated vertices)
 3. Circuit := circuit C "spliced" with sub-circuit sc
4. Circuit C has the Euler circuit.

Representation- Incidence Matrix

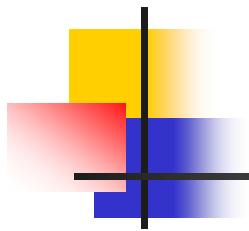


	e_1	e_2	e_3	e_4	e_5	e_6	e_7
a	1	0	0	0	0	0	1
b	1	1	0	0	0	0	0
c	0	1	1	0	1	1	0
d	0	0	1	1	0	0	0
e	0	0	0	1	1	0	0
f	0	0	0	0	0	1	1



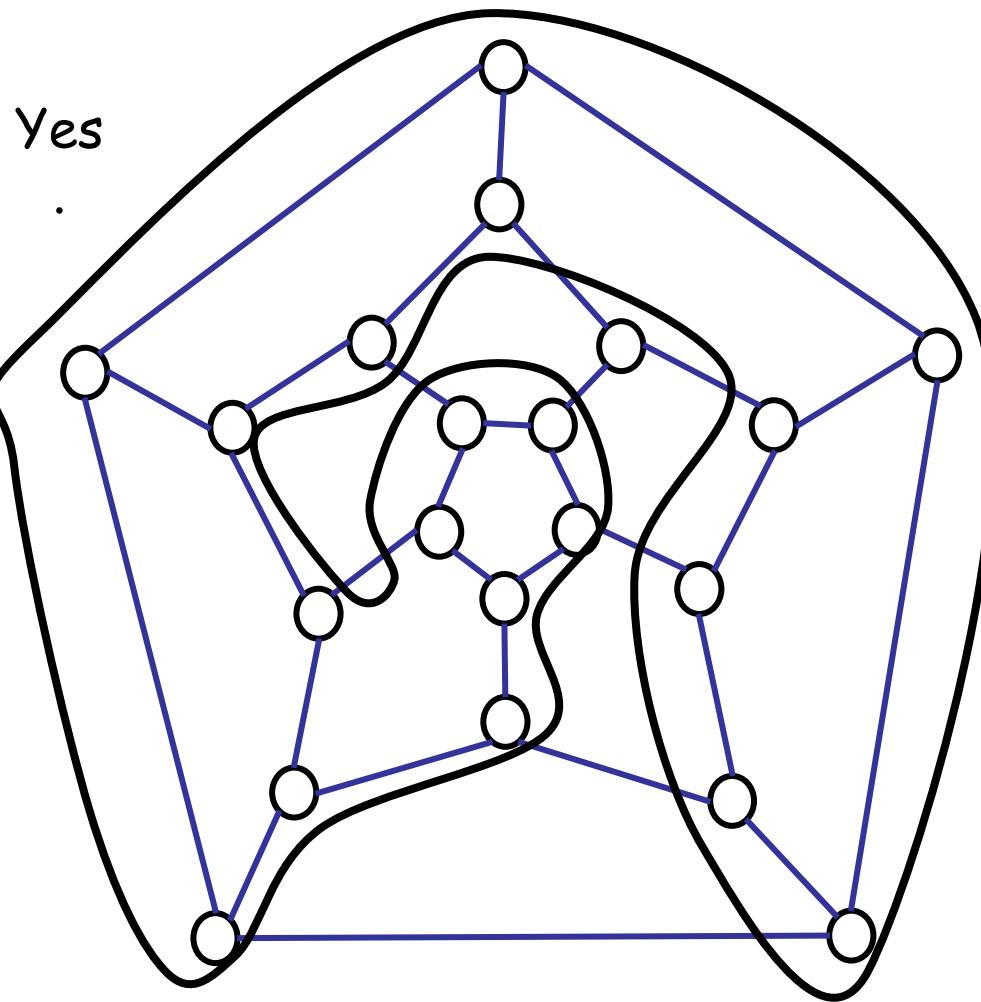
Hamiltonian Graph

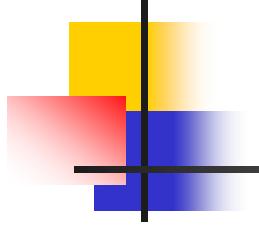
- **Hamiltonian path** (also called *traceable path*) is a path that visits each vertex exactly once.
- A **Hamiltonian cycle** (also called *Hamiltonian circuit*, *vertex tour* or *graph cycle*) is a cycle that visits each vertex exactly once (except for the starting vertex, which is visited once at the start and once again at the end).
- A graph that contains a Hamiltonian path is called a **traceable graph**. A graph that contains a Hamiltonian cycle is called a **Hamiltonian graph**. Any Hamiltonian cycle can be converted to a Hamiltonian path by removing one of its edges, but a Hamiltonian path can be extended to Hamiltonian cycle only if its endpoints are adjacent.



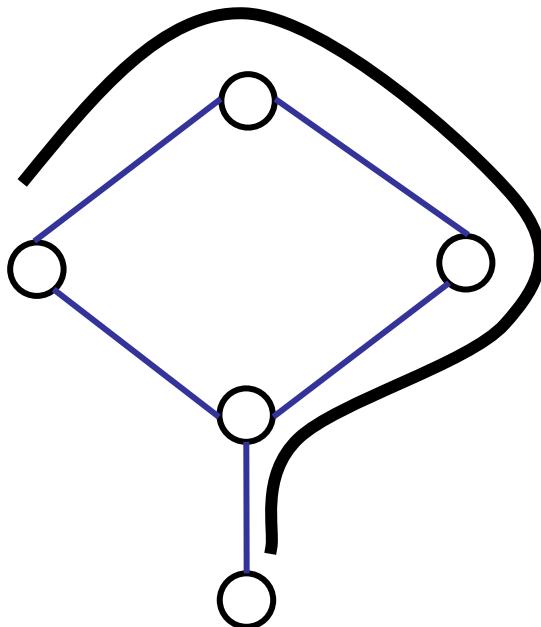
A graph of the vertices of a dodecahedron.

Is it Hamiltonian?

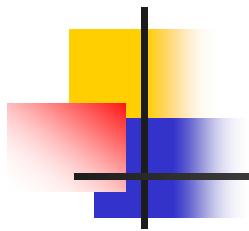




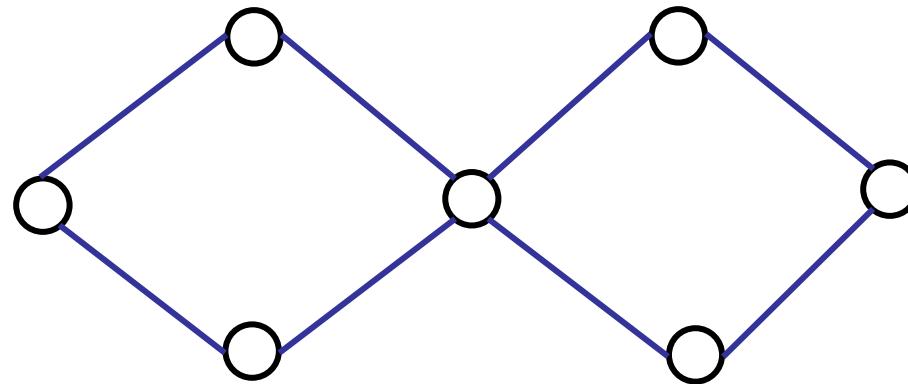
Hamiltonian Graph



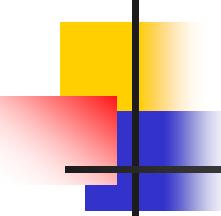
This one has a Hamiltonian path, but not a Hamiltonian tour.



Hamiltonian Graph

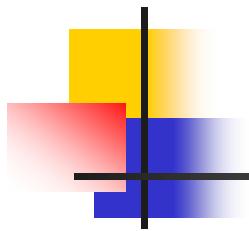


This one has an Euler tour, but no Hamiltonian path.



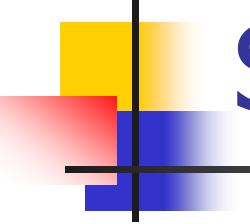
Hamiltonian Graph

- Similar notions may be defined for directed graphs, where edges (arcs) of a path or a cycle are required to point in the same direction, i.e., connected tail-to-head.
- The *Hamiltonian cycle problem* or *Hamiltonian circuit problem* in graph theory is to find a Hamiltonian cycle in a given graph. The *Hamiltonian path problem* is to find a Hamiltonian path in a given graph.
- There is a simple relation between the two problems. The Hamiltonian path problem for graph **G** is equivalent to the Hamiltonian cycle problem in a graph **H** obtained from **G** by adding a new vertex and connecting it to all vertices of **G**.
- Both problems are NP-complete. However, certain classes of graphs always contain Hamiltonian paths. For example, it is known that every tournament has an odd number of Hamiltonian paths.



Hamiltonian Graph

- **DIRAC'S Theorem:** if G is a simple graph with n vertices with $n \geq 3$ such that the degree of every vertex in G is at least $n/2$ then G has a Hamilton circuit.
- **ORE'S Theorem:** if G is a simple graph with n vertices with $n \geq 3$ such that $\deg(u) + \deg(v) \geq n$ for every pair of nonadjacent vertices u and v in G , then G has a Hamilton circuit.

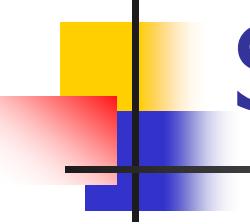


Shortest Path

- Generalize distance to weighted setting
- Digraph $G = (V, E)$ with weight function $W: E \rightarrow R$ (assigning real values to edges)
- Weight of path $p = v_1 \rightarrow v_2 \rightarrow \dots \rightarrow v_k$ is

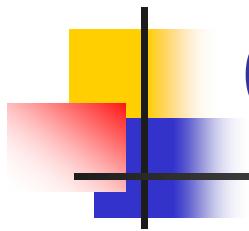
$$w(p) = \sum_{i=1}^{k-1} w(v_i, v_{i+1})$$

- Shortest path = a path of the minimum weight
- Applications
 - static/dynamic network routing
 - robot motion planning
 - map/route generation in traffic



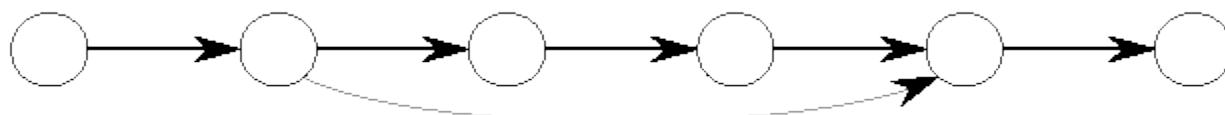
Shortest-Path Problems

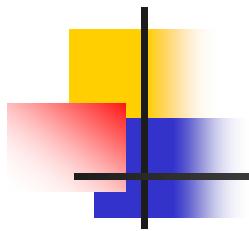
- Shortest-Path problems
 - **Single-source (single-destination).** Find a shortest path from a given source (vertex s) to each of the vertices. The topic of this lecture.
 - **Single-pair.** Given two vertices, find a shortest path between them. Solution to single-source problem solves this problem efficiently, too.
 - **All-pairs.** Find shortest-paths for every pair of vertices. Dynamic programming algorithm.
 - Unweighted shortest-paths – BFS.



Optimal Substructure

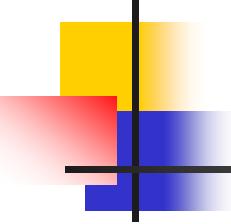
- *Theorem:* subpaths of shortest paths are shortest paths
- Proof ("cut and paste")
 - if some subpath were not the shortest path, one could substitute the shorter subpath and create a shorter total path





Negative Weights and Cycles?

- Negative edges are OK, as long as there are no *negative weight cycles* (otherwise paths with arbitrary small “lengths” would be possible)
- Shortest-paths can have no cycles (otherwise we could improve them by removing cycles)
 - Any shortest-path in graph G can be no longer than $n - 1$ edges, where n is the number of vertices

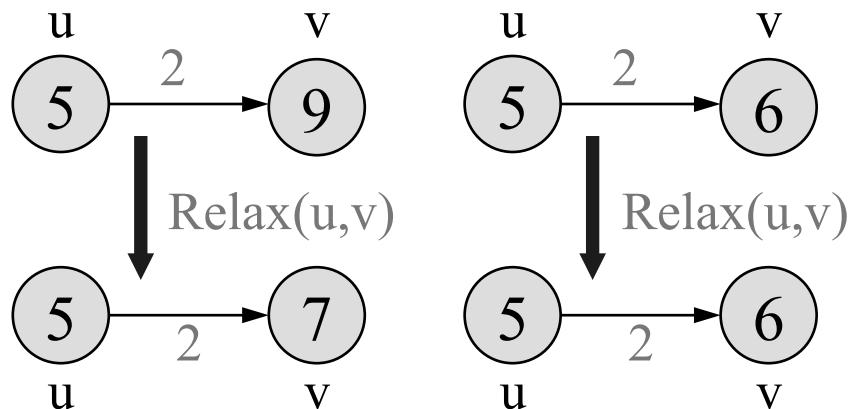


Shortest Path Tree

- The result of the algorithms – a *shortest path tree*. For each vertex v , it
 - records a shortest path from the start vertex s to v .
 $v.\text{parent}()$ gives a predecessor of v in this shortest path
 - gives a shortest path length from s to v , which is recorded in $v.\text{d}()$.
- The same pseudo-code assumptions are used.
- **Vertex** ADT with operations:
 - **adjacent()**: VertexSet
 - **d():int** and **setd(k:int)**
 - **parent():Vertex** and **setparent(p:Vertex)**

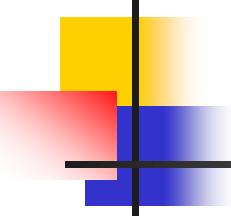
Relaxation

- For each vertex v in the graph, we maintain $v.d()$, the estimate of the shortest path from s , initialized to ∞ at the start
- Relaxing an edge (u,v) means testing whether we can improve the shortest path to v found so far by going through u



Relax

```
( $u, v, G$ )
if  $v.d() > u.d() + G.w(u, v)$  then
     $v.setd(u.d() + G.w(u, v))$ 
     $v.setParent(u)$ 
```



Dijkstra's Algorithm

- Non-negative edge weights
- Greedy, similar to Prim's algorithm for MST
- Like breadth-first search (if all weights = 1, one can simply use BFS)
- Use Q , a priority queue ADT keyed by $v.d()$ (BFS used FIFO queue, here we use a PQ, which is re-organized whenever some d decreases)
- Basic idea
 - maintain a set S of solved vertices
 - at each step select "closest" vertex u , add it to S , and relax all edges from u

Dijkstra's ALgorithm

Solution to **Single-source (single-destination)**.

- Input: Graph G , start vertex s

Dijkstra (G, s)

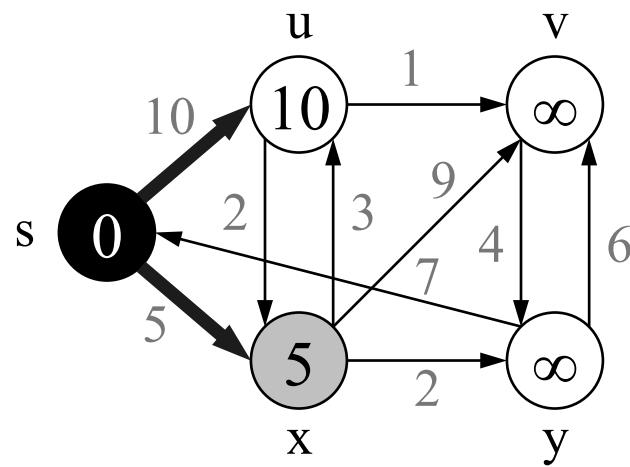
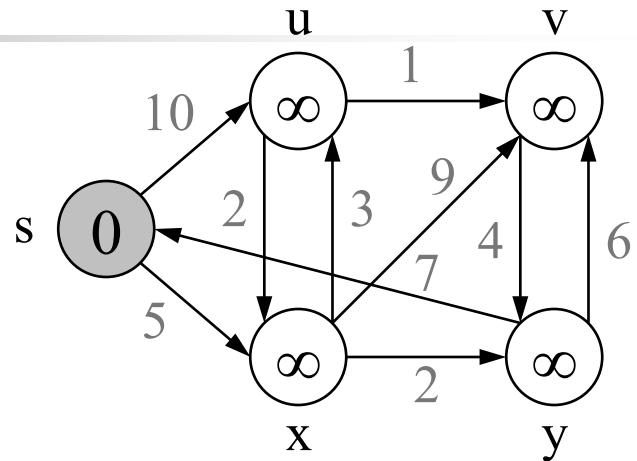
```
01 for each vertex  $u \in G.V()$ 
02      $u.setd(\infty)$ 
03      $u.setParent(NIL)$ 
04  $s.setd(0)$ 
05  $S \leftarrow \emptyset$                                 // Set  $S$  is used to explain the
                                                algorithm
06  $Q.init(G.V())$     //  $Q$  is a priority queue ADT
07 while not  $Q.isEmpty()$ 
08      $u \leftarrow Q.extractMin()$ 
09      $S \leftarrow S \cup \{u\}$                                 relaxing
10     for each  $v \in u.adjacent()$  do                  edges
11         Relax ( $u, v, G$ )
12          $Q.modifyKey(v)$ 
```

Dijkstra's Example

Dijkstra(G, s)

```

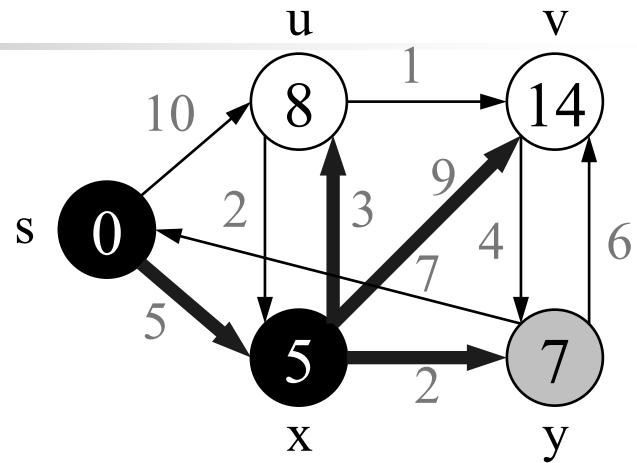
01 for each vertex  $u \in G.V()$ 
02      $u.setd(\infty)$ 
03      $u.setParent(NIL)$ 
04  $s.setd(0)$ 
05  $S \leftarrow \emptyset$ 
06  $Q.init(G.V())$ 
07 while not  $Q.isEmpty()$ 
08      $u \leftarrow Q.extractMin()$ 
09      $S \leftarrow S \cup \{u\}$ 
10    for each  $v \in u.adjacent()$  do
11        Relax( $u, v, G$ )
12         $Q.modifyKey(v)$ 
```



Dijkstra's Example

```
Dijkstra(G, s)
```

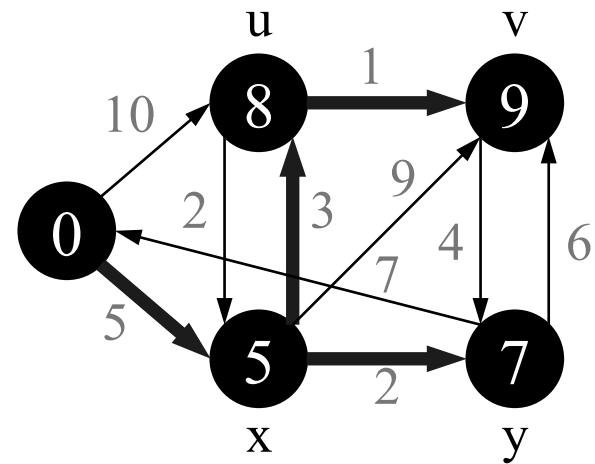
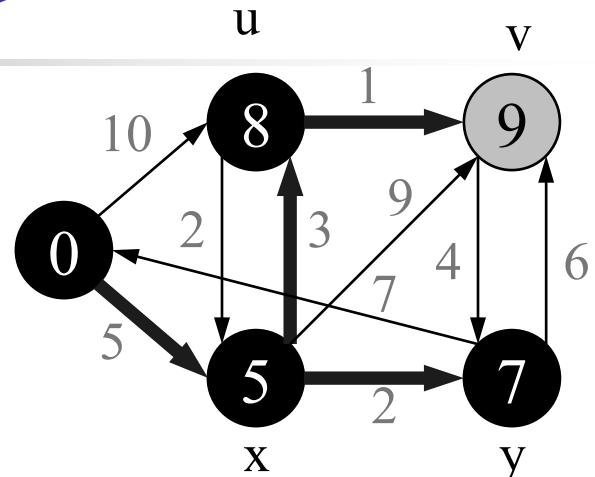
```
01 for each vertex u ∈ G.V()
02     u.setd(∞)
03     u.setParent(NIL)
04 s.setd(0)
05 S ← ∅
06 Q.init(G.V())
07 while not Q.isEmpty()
08     u ← Q.extractMin()
09     S ← S ∪ {u}
10    for each v ∈ u.adjacent() do
11        Relax(u, v, G)
12        Q.modifyKey(v)
```

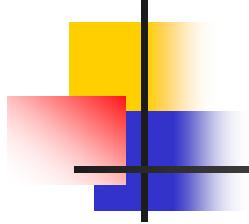


Dijkstra's Example

```
Dijkstra(G, s)
```

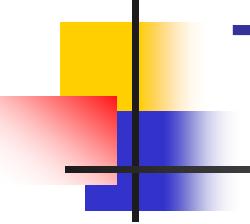
```
01 for each vertex u  $\in G.V()$ 
02     u.setd( $\infty$ )
03     u.setParent(NIL)
04 s.setd(0)
05 S  $\leftarrow \emptyset$ 
06 Q.init(G.V())
07 while not Q.isEmpty()
08     u  $\leftarrow$  Q.extractMin()
09     S  $\leftarrow S \cup \{u\}$ 
10    for each v  $\in u.adjacent()$  do
11        Relax(u, v, G)
12        Q.modifyKey(v)
```





Dijkstra's Algorithm

- $O(n^2)$ operations
 - $(n-1)$ iterations: 1 for each vertex added to the distinguished set S .
 - $(n-1)$ iterations: for each adjacent vertex of the one added to the distinguished set.
- Note: it is single source – single destination algorithm



Traveling Salesman Problem

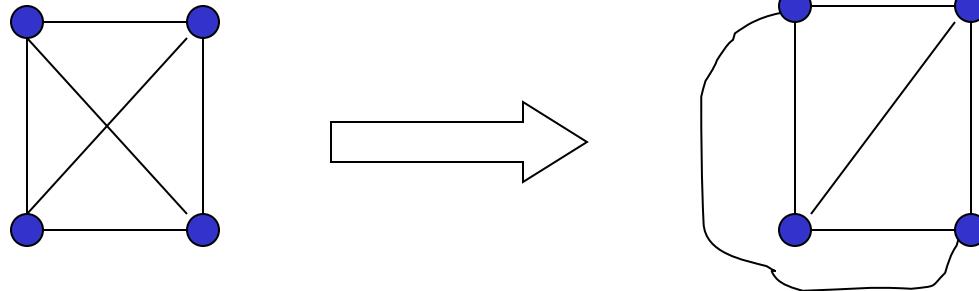
- Given a number of cities and the costs of traveling from one to the other, what is the cheapest roundtrip route that visits each city once and then returns to the starting city?
- An equivalent formulation in terms of graph theory is: Find the Hamiltonian cycle with the least weight in a weighted graph.
- It can be shown that the requirement of returning to the starting city does not change the computational complexity of the problem.
- A related problem is the (bottleneck TSP): Find the Hamiltonian cycle in a weighted graph with the minimal length of the longest edge.

Planar Graphs

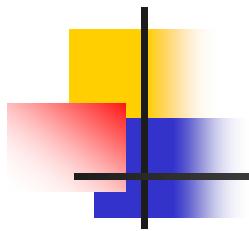
- A graph (or multigraph) G is called *planar* if G can be drawn in the plane with its edges intersecting only at vertices of G , such a drawing of G is called an *embedding* of G in the plane.

Application Example: VLSI design (overlapping edges requires extra layers), Circuit design (cannot overlap wires on board)

Representation examples: K_1, K_2, K_3, K_4 are planar, K_n for $n > 4$ are non-planar

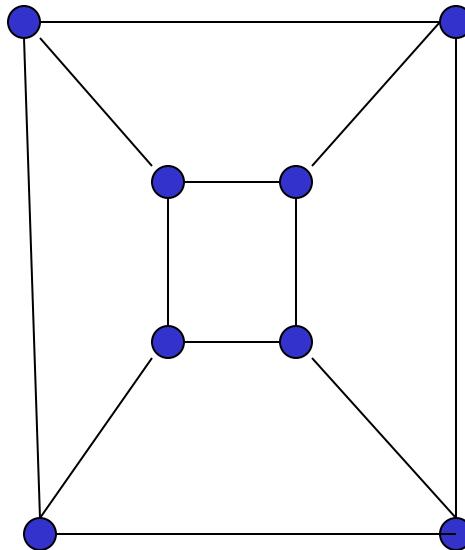
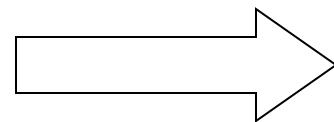
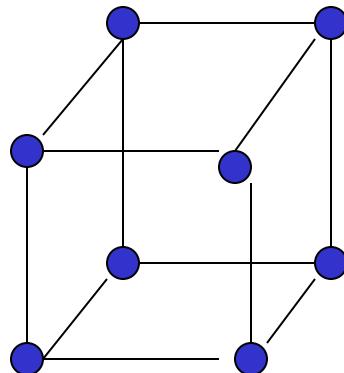


K_4



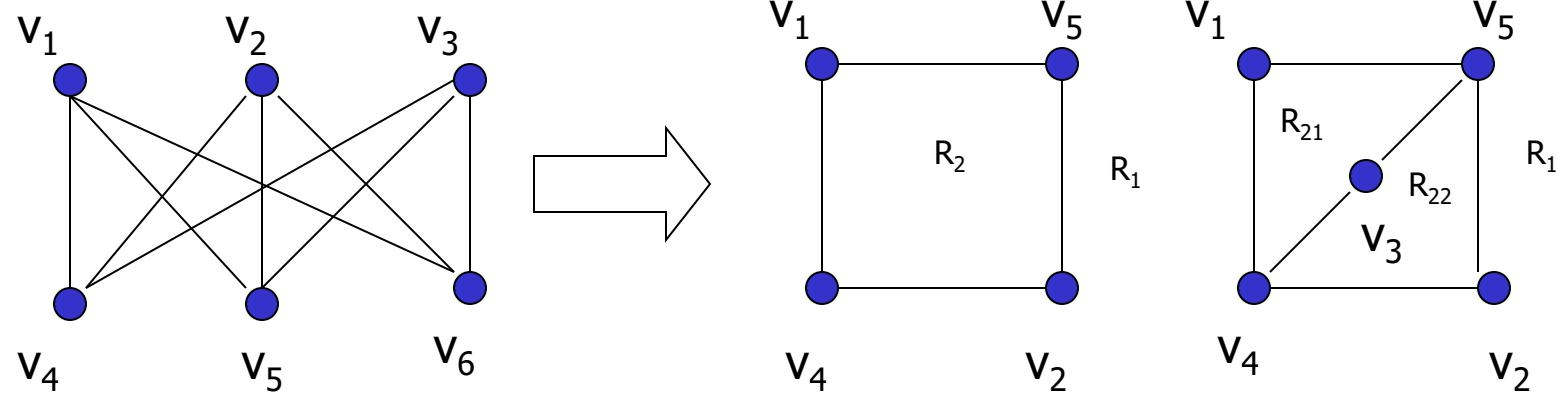
Planar Graphs

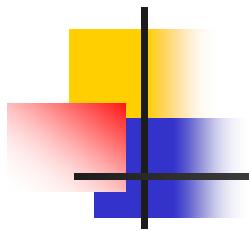
- Representation examples: Q_3



Planar Graphs

- Representation examples: $K_{3,3}$ is Nonplanar

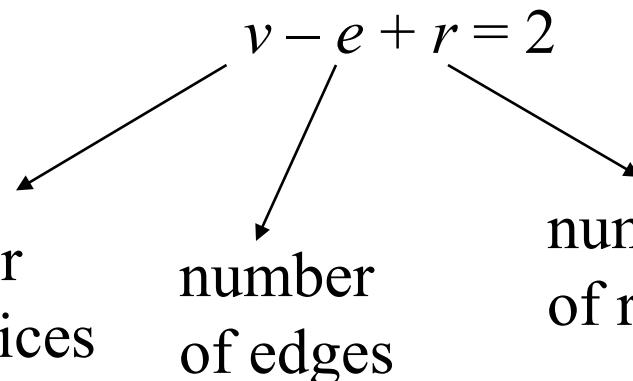




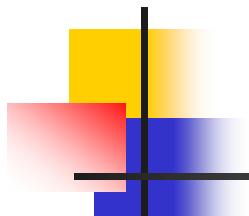
Planar Graphs

Theorem : *Euler's planar graph theorem*

For a **connected** planar graph or multigraph:

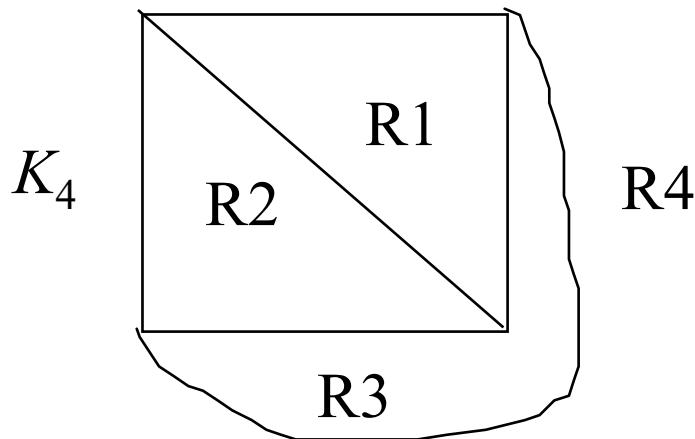
$$v - e + r = 2$$


The diagram illustrates the Euler formula $v - e + r = 2$ for a connected planar graph. The formula is at the top, with three arrows pointing downwards to three labels below it. The first arrow points to the term v , which is followed by the text "number of vertices". The second arrow points to the term e , which is followed by the text "number of edges". The third arrow points to the term r , which is followed by the text "number of regions".



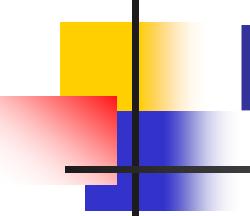
Planar Graphs

Example of Euler's theorem



A planar graph divides the plane into several regions (faces), one of them is the infinite region.

$$v=4, e=6, r=4, v-e+r=2$$



Planar Graphs

- Proof of Euler's formula: By Induction
Base Case: for G_1 , $e_1 = 1$, $v_1 = 2$ and $r_1 = 1$

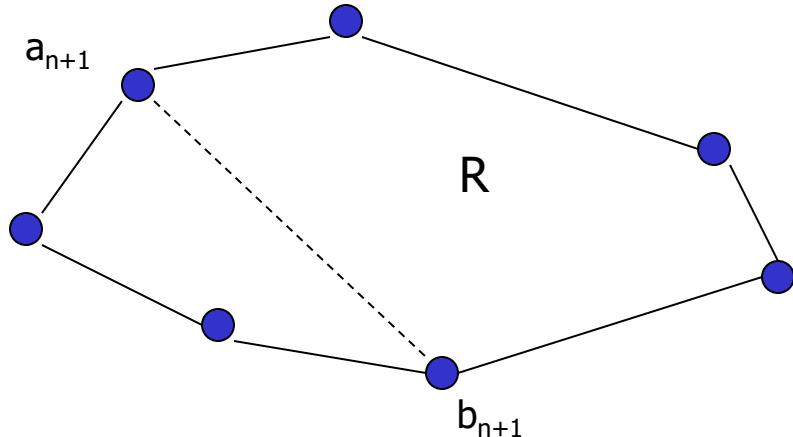


n+1 Case: Assume, $r_n = e_n - v_n + 2$ is true. Let $\{a_{n+1}, b_{n+1}\}$ be the edge that is added to G_n to obtain G_{n+1} and we prove that $r_n = e_n - v_n + 2$ is true. Can be proved using two cases.

Planar Graphs

- Case 1:

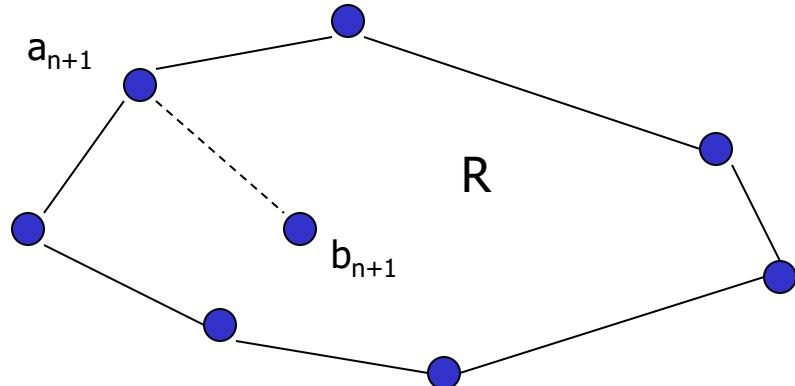
$$r_{n+1} = r_n + 1, e_{n+1} = e_n + 1, v_{n+1} = v_n \Rightarrow r_{n+1} = e_{n+1} - v_{n+1} + 2$$



Planar Graphs

- Case 2:

$$r_{n+1} = r_n, e_{n+1} = e_n + 1, v_{n+1} = v_n + 1 \Rightarrow r_{n+1} = e_{n+1} - v_{n+1} + 2$$



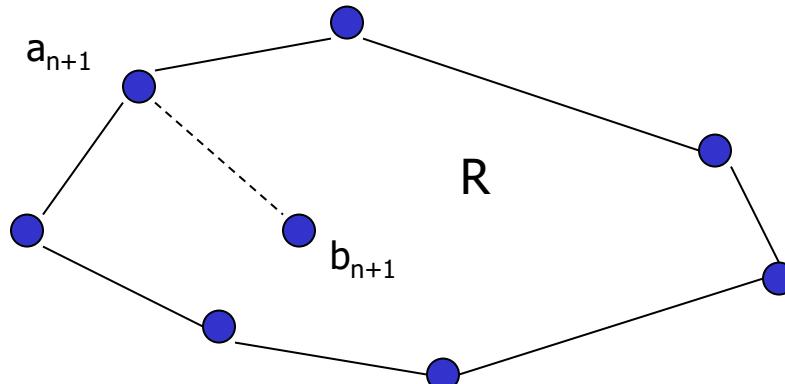
Planar Graphs

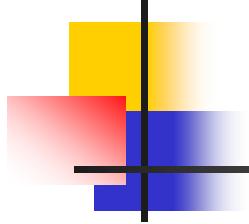
Corollary 1: Let $G = (V, E)$ be a connected simple planar graph with $|V| = v$, $|E| = e > 2$, and r regions. Then $3r \leq 2e$ and $e \leq 3v - 6$

Proof: Since G is loop-free and is not a multigraph, the boundary of each region (including the infinite region) contains at least three edges. Hence, each region has degree ≥ 3 .

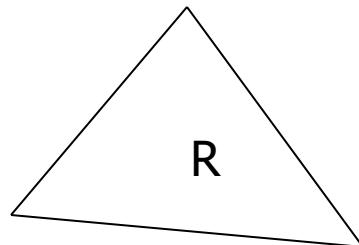
Degree of region: No. of edges on its boundary; 1 edge may occur twice on boundary \rightarrow contributes 2 to the region degree.

Each edge occurs exactly twice: either in the same region or in 2 different regions

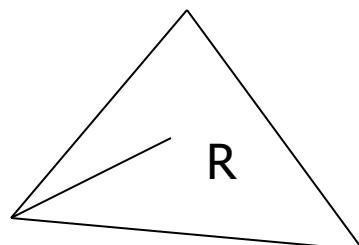




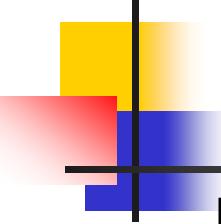
Region Degree



Degree of R = 3



Degree of R = ?



Planar Graphs

Each edge occurs exactly twice: either in the same region or in 2 different regions

$\Rightarrow 2e = \text{sum of degree of } r \text{ regions determined by } 2e$

$\Rightarrow 2e \geq 3r.$ (since each region has a degree of at least 3)

$\Rightarrow r \leq (2/3) e$

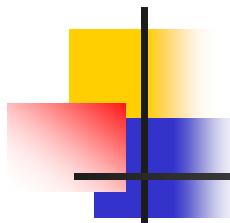
\Rightarrow From Euler's theorem, $2 = v - e + r$

$\Rightarrow 2 \leq v - e + 2e/3$

$\Rightarrow 2 \leq v - e/3$

\Rightarrow So $6 \leq 3v - e$

\Rightarrow or $e \leq 3v - 6$



Planar Graphs

Corollary 2: Let $G = (V, E)$ be a connected simple planar graph then G has a vertex degree that does not exceed 5

Proof: If G has one or two vertices the result is true

If G has 3 or more vertices then by Corollary 1, $e \leq 3v - 6$

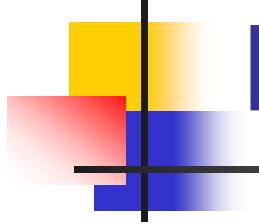
$$\Rightarrow 2e \leq 6v - 12$$

If the degree of every vertex were at least 6:

by Handshaking theorem: $2e = \text{Sum}(\deg(v))$

$$\Rightarrow 2e \geq 6v. \text{ But this contradicts the inequality } 2e \leq 6v - 12$$

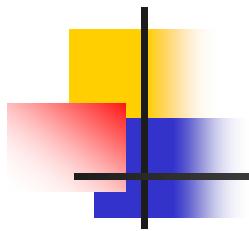
\Rightarrow There must be at least one vertex with degree no greater than 5



Planar Graphs

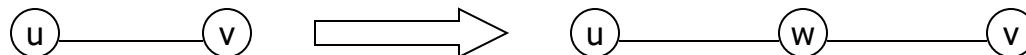
Corollary 3: Let $G = (V, E)$ be a connected simple planar graph with v vertices ($v \geq 3$), e edges, and no circuits of length 3 then $e \leq 2v - 4$

Proof: Similar to Corollary 1 except the fact that no circuits of length 3 imply that degree of region must be at least 4.



Planar Graphs

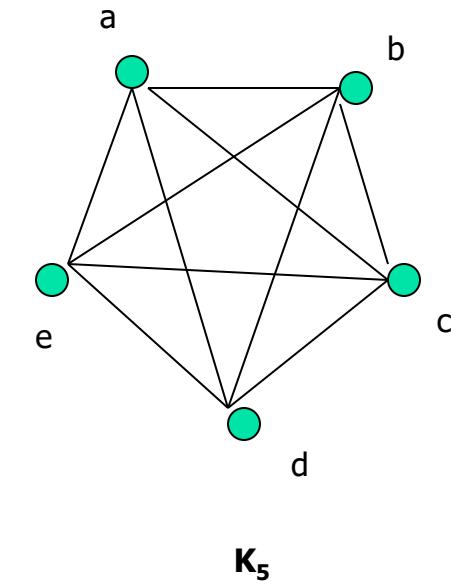
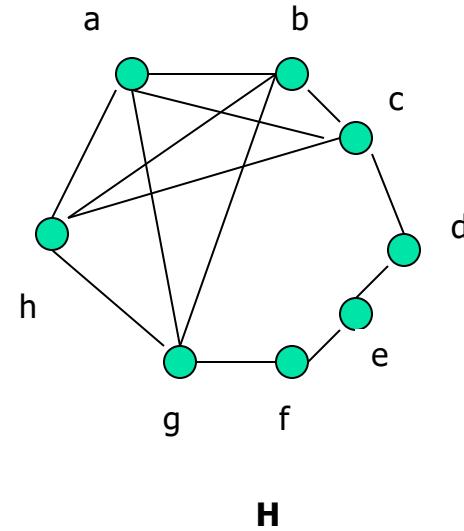
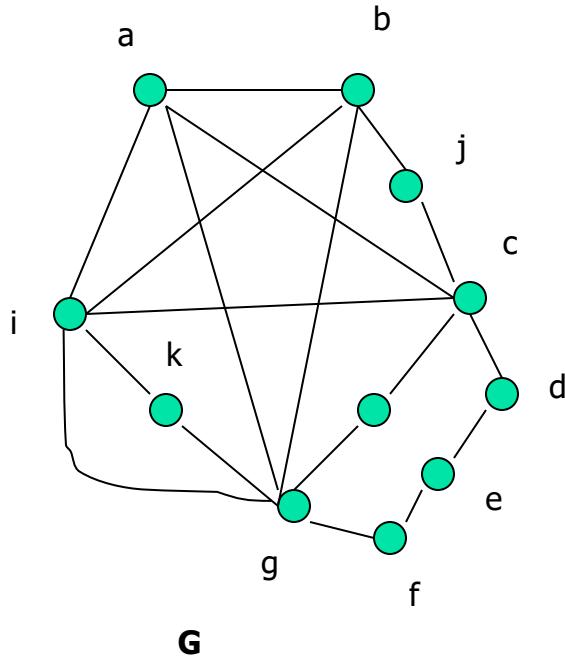
- **Elementary sub-division:** Operation in which a graph are obtained by removing an edge $\{u, v\}$ and adding the vertex w and edges $\{u, w\}, \{w, v\}$

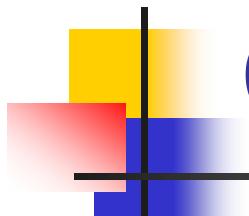


- **Homeomorphic Graphs:** Graphs G1 and G2 are termed as homeomorphic if they are obtained by sequence of elementary sub-divisions.

Planar Graphs

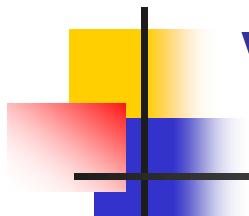
- **Kuratowski's Theorem:** A graph is non-planar if and only if it contains a subgraph homeomorphic to $K_{3,3}$ or K_5
Representation Example: G is Nonplanar





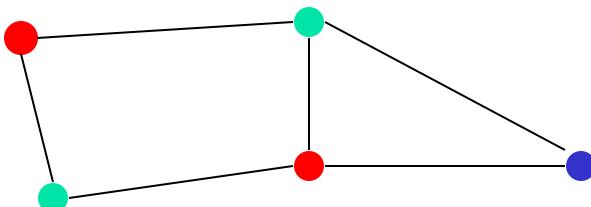
Graph Coloring Problem

- **Graph coloring** is an assignment of "*colors*", almost always taken to be consecutive integers starting from 1 without loss of generality, to certain objects in a graph. Such objects can be vertices, edges, faces, or a mixture of the above.
- Application examples: scheduling, register allocation in a microprocessor, frequency assignment in mobile radios, and pattern matching



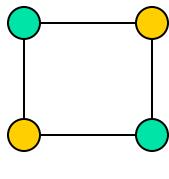
Vertex Coloring Problem

- Assignment of colors to the vertices of the graph such that proper coloring takes place (no two adjacent vertices are assigned the same color)
- **Chromatic number:** least number of colors needed to color the graph
- A graph that can be assigned a (proper) k -coloring is **k -colorable**, and it is **k -chromatic** if its chromatic number is exactly k .

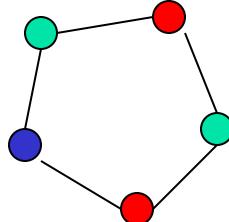


Vertex Coloring Problem

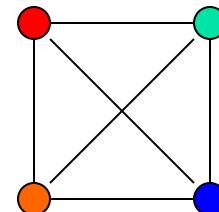
- The problem of finding a minimum coloring of a graph is NP-Hard
- The corresponding decision problem (Is there a coloring which uses at most k colors?) is NP-complete
- The chromatic number for $C_n = 3$ (n is odd) or 2 (n is even), $K_n = n$, $K_{m,n} = 2$
- C_n : cycle with n vertices; K_n : fully connected graph with n vertices; $K_{m,n}$: complete bipartite graph



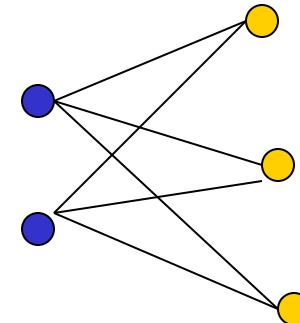
C_4



C_5



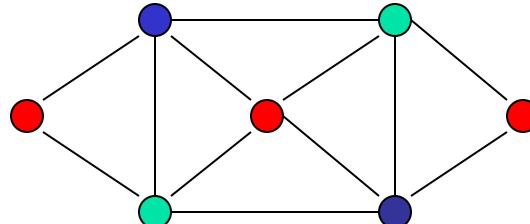
K_4



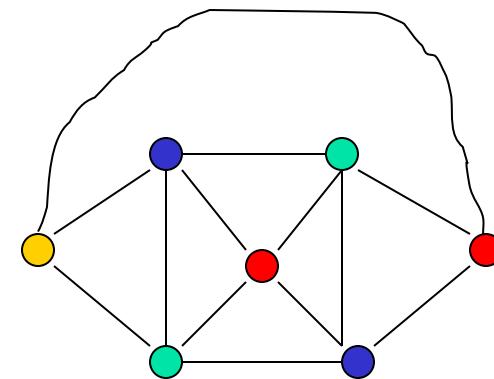
$K_{2,3}$

Vertex Covering Problem

- **The Four color theorem:** the chromatic number of a planar graph is no greater than 4
- Example: G1 chromatic number = 3, G2 chromatic number = 4
- (Most proofs rely on case by case analysis).



G1



G2

Algebraic Systems

Need to study Algebraic systems:

- Algebraic Model : Real Worlds Situation, Mathematical model, connecting mathematical model with real world situation to get real world solution.

Algebraic Systems or Algebras

- **Structure / Definition:** An algebra is characterised by specifying 3 components
 - a **set** called **Carrier** of the Algebra
 - **Operations** defined on the carrier
 - **Distinguished** elements of the carrier, called **constants** of the algebra
- **Example:** let carrier be Set of integers Z and define operation + (addition) on Z
 - it means if a and b are integers, then you can perform $a + b$
 - this operation is from $I^2 \rightarrow I$, it's a binary operation

Contd...

- In general, let carrier be S
 - then an operation from $S^m \rightarrow S$
 - here m is called as **arity of the operation**
 - Example:
 - Binary operations:
 - Multiplication *
 - Subtraction -
 - Unary Operation
 - Negation –
 - absolute value or Mod

Contd...

- **Constants of algebra:** elements of the carrier having some special property
 - **Example:** $(\mathbb{I}, +, 0)$
 - 0 is identity element for addition
 - **Example:** $(\mathbb{R}, *, 0, 1)$
 - 1 is identity element for Multiplication
 - 0 is Zero element for multiplication
- **Fundamental Algebraic Structures:** groupoids, semi-groups, monoids, groups, lattices, rings and fields.

Algebras of same signature or from same species

- Algebras are said to have same signature if they have
 1. A Carrier
 2. Same number of operations with corresponding arity
 3. same number of constants

- **Example 1:**
 - $\langle I, +, *, -, 1, 0 \rangle$
 - $\langle R, +, *, -, 1, 0 \rangle$
 - $\langle P(S), \cup, \cap, ', S, \emptyset \rangle$
- The above algebras have same signatures, or they are from same species
- **Example 2:**
 - $\langle I, -, 0 \rangle$ and $\langle Q, +, 0 \rangle$
 - Here the above algebras do have same signature, but they do not have same properties

Axioms

- **Axioms** are rules that algebras follow.
 - **Example:** Semi groups will follow a set of axioms, groups will follow a set of operations

Closure Property

- **Definition:** let \circ and Δ be a binary and unary operation on a set T and let T' be a subset of T . T' is closed with respect to \circ if $a, b \in T$ implies $a \circ b \in T'$. The subset T' is closed with respect to Δ if $a \in T$ implies $\Delta a \in T'$.
- **Example:** $\langle \mathbb{I}, +, 0 \rangle$
 - Let $S = \{x \mid 0 \leq x \leq 10\}$
 - here, $12 + 15 = 27$ which does not belong to S
so, S is not closed wrt $+$
 - Consider operation $\max(a, b)$
 - here S is closed under \max operation

Contd...

- **Example 2:** Let If $A = \{0, 1\}$,
 - We have
 - $0 \times 0 = 0$,
 - $0 \times 1 = 0$,
 - $1 \times 0 = 0$, and
 - $1 \times 1 = 1$
 - so A is closed under multiplication.
 - But A is not closed under the binary operation addition. Since $1 + 1 = 2$ does not belong to A .

Groupoid

- **Definition:** A groupoid is an algebraic structure consisting of non-empty set A and a binary operation *, such that A is closed under *.
- **Example:** The set of real numbers is closed under addition, therefore $(\mathbb{R}, +)$ is a groupoid.
- **Example 2:** If E denotes the set of even numbers then E is closed under addition. and $(E, +)$ is a groupoid.
- **Example 3:** Let \mathbb{Z}^+ denotes the set of positive integers and * be a binary operation on \mathbb{Z}^+ defined as

$$a * b = 3a + 4b \quad \forall a, b \in \mathbb{Z}^+$$

Clearly $(\mathbb{Z}^+, *)$ is a groupoid

Semi-Group

- **Definition:** Let S be a non-empty set and $*$ be a binary operation on S . The algebra $(S, *)$ is called a semi-group if the operation $*$ is associative.
 - In other words, the groupoid is a semi-group if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$
- Thus, a semi-group requires the following:
 - (i) A set S .
 - (ii) A binary operation $*$ defined on the elements of S .
 - (iii) Closure, $a * b$ whenever $a, b \in S$
 - (iv) Associativity $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$
- **Example 1:** Let N be the set of natural numbers. Then $(N, +)$ and $(N, *)$ are semi-groups.

Contd...

- **Example 2:** X be a non-empty set and P (X) denote the power set of X. Then $(P(x), \cup)$ and $(P (x), \cap)$ are semi-groups.
- **Example 3:** Let Z be the set of integers and Z_m be the set equivalence classes generated by the equivalence relation “congruent modulo M” for any positive integers m. Then $+_m$ be defined integers of + on Z as follows:

For any $[i], [j] \in Z_m$

$$[i] +_m [j] = [(i + j) \text{ mod } m]$$

The algebraic system $(Z_m, +_m)$ is a semi-group

Homomorphism of Semi-Groups

- **Definition:** Let $(S, *)$ and (T, o) be any two semi-groups. A mapping $f: S \rightarrow T$ such that for any two elements $a, b \in S$

$$f(a * b) = f(a) o f(b)$$

is called a semi-group homomorphism.

- **Definition:** A homomorphism of a semi-group into itself is called a semi-group **endomorphism**.

Isomorphism of Semi-Group

- **Definition:** Let $(S, *)$ and $(T, 0)$ be any two semi-groups. A homomorphism $f: S \rightarrow T$ is called a semi-group isomorphism if f is one-to-one and onto.
- If $f: S \rightarrow T$ is an isomorphism then $(S, *)$ and $(T, 0)$ are said to be isomorphic.
- **Definition:** An isomorphism of a semi-group onto itself is called a semi-group automorphism.

Monoid

- **Definition:** A semi-group $(M, *)$ with an identity element with respect to the binary operation $*$ is called a monoid.
- In other words, an algebraic system $(M, *)$ is called a monoid if:
 - (i) $(a * b) * c = a * (b * c) \quad \forall a, b, c \in M$
 - (ii) There exists an element $e \in M$ such that $e * a = a * e = a \quad \forall a \in M$. (i.e. Identity Element)
- **Example 1:** Let Z be the set of integers $(Z, +)$ is a monoid 0 is the identity element in Z with respect to $+$.

Contd...

- **Commutative Monoid:** Let $(M, *)$ be a monoid. If the operation $*$ is commutative then $(M, *)$ is said to be commutative monoid.
- If $a^i a^j \in M$ we have $a^{i+j} = a^i * a^j = a^j * a^i$ for all $i, j \in M$.
- **Cyclic Monoid:** A monoid $(M, *)$ is said to be cyclic if there exists an element $a \in M$. Such that every element of M can be expressed as some power of a .
 - If M is a cyclic monoid such that every element is some power of $a \in M$, then a is called the generator of M .
 - A cyclic monoid is commutative and may have more than one generator.

Monoid Homomorphism

- **Definition:** Let $(M, *)$ and $(T, 0)$ be any two monoids e_m and e_t denote the identity elements of $(M, *)$ and $(T, 0)$ respectively. A mapping

$$f: M \rightarrow T$$

such that for any two elements $a, b \in M$

$$f(a * b) = f(a) \circ f(b)$$

and $f(e_m) = e_t$

is called a monoid homomorphism.

- Monoid homomorphism preserves the associativity and identity.
- It also preserves commutative.
- If $a \in M$ is invertible and $a^{-1} \in M$ is the inverse of a in M , then $f(a^{-1})$ is the inverse of $f(a)$, i.e., $f(a^{-1}) = [f(a)]^{-1}$.

Groups

- **Definition:** A group is an algebraic structure $(G, *)$ in which the binary operation $*$ on G satisfies the following conditions:

G – 1 for all $a, b, c, \in G$

$a * (b * c) = (a * b) * c$ (**associativity**)

G – 2 there exists an elements $e G \in$ such that for any $a G \in$

$a * e = e * a = a$ (**existence of identity**)

G – 3 for every $a \in G$, there exists an element denoted by a^{-1} in G

such that

$a * a^{-1} = a^{-1} * a = e$

a^{-1} is called the **inverse** of a in G

Contd...

- **Example 1:** $(\mathbb{Z}, +)$ is a group
 - where \mathbb{Z} denote the set of integers.
- **Example 2:** $(\mathbb{R}, +)$ is a group
 - where \mathbb{R} denote the set of real numbers.

Abelian Group

- **Definition:** Let $(G, *)$ be a group. If $*$ is commutative that is $a * b = b * a$ for all $a, b \in G$ then $(G, *)$ is called an Abelian group.
- **Example:** $(\mathbb{Z}, +)$ is an Abelian group

Finite and Infinite Group

- **Finite Group**

- **Definition:** A group G is said to be a finite group if the set G is a finite set.
- **Example:** $G = \{-1, 1\}$ is a group with respect to the operation multiplication. Where G is a finite set having 2 elements. Therefore, G is a finite group.

- **Infinite Group**

- A group G , which is not finite is called an infinite group.

Order of a Finite Group

- **Definition:** The order of a finite group $(G, *)$ is the number of distinct elements in G .
- The order of G is denoted by $O(G)$ or by $|G|$.

- **Example:** Let $G = \{-1, 1\}$

The set G is a group with respect to the binary operation multiplication and $O(G) = 2$.

Example 1

- Show that the set $G = \{1, -1, i, -i\}$ where $i = \sqrt{-1}$ is an abelian group with respect to multiplication as a binary operation.
- **Solution:** Let us construct the composition table

•	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

- From the table we can say (G, \cdot) is closed under the \cdot operation

Contd...

- We have to check whether the above algebraic structure (G, \cdot) satisfies the following axioms
- Associativity

$$1 \cdot (-1 \cdot i) = 1 \cdot -i = -i$$

$$(1 \cdot -1) \cdot i = -1 \cdot i = -i$$

$$\Rightarrow 1 \cdot (-1 \cdot i) = (1 \cdot -1) i$$

- Existence of Identity
 - 1 is identity element of (G, \cdot) such that $1 \cdot a = a = a \cdot 1 \quad \forall a \in G$

Contd...

- Existence of inverse

$$1 \cdot 1 = 1 = 1 \cdot 1 \Rightarrow 1 \text{ is inverse of } 1$$

$$(-1) \cdot (-1) = 1 = (-1) \cdot (-1) \Rightarrow -1 \text{ is the inverse of } (-1)$$

$$i \cdot (-i) = 1 = -i \cdot i \Rightarrow -i \text{ is the inverse of } i \text{ in } G.$$

$$-i \cdot i = 1 = i \cdot (-i) \Rightarrow i \text{ is the inverse of } -i \text{ in } G.$$

- Thus all the axioms of a group are satisfied.

Contd...

- Commutativity

$$a \cdot b = b \cdot a \quad \forall a, b \in G \text{ hold in } G$$

$$1 \cdot 1 = 1 = 1 \cdot 1, -1 \cdot 1 = -1 = 1 \cdot -1$$

$$i \cdot 1 = i = 1 \cdot i; i \cdot -i = -i \cdot i = 1 = 1 \text{ etc.}$$

commutative law is satisfied

- Hence (G, \cdot) is an abelian group

Example 2

- Prove that $G = \{1, \omega, \omega^2\}$ is a group with respect to multiplication where $1, \omega, \omega^2$ are cube roots of unity.
- **Solution:** We construct the composition table as follows:

•	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	$\omega^3 = 1$
ω^2	ω^2	$\omega^3 = 1$	$\omega^4 = \omega$

- The algebraic system is (G, \cdot) where $\omega^3 = 1$ and multiplication \cdot is the binary operation on G .
- The algebraic system (G, \cdot) is closed under multiplication “ \cdot ”.

Contd...

- Let us check axioms of groups
 - Associativity
 - from the table we can say \cdot is associative
 - Existence of Identity
 - 1 is identity element of (G, \cdot) such that
$$1 \cdot a = a = a \cdot 1 \quad \forall a \in G$$
 - Existence of inverse
 - Each element of G is invertible
 - $1 \cdot 1 = 1 \Rightarrow 1$ is its own inverse.
 - $\omega \cdot \omega^2 = \omega^3 = 1 \Rightarrow \omega^2$ is the inverse of ω and ω is the inverse of ω^2 in G
- Thus all the axioms of a group are satisfied.
- Commutativity
 - commutative law hold wrt multiplication
- Hence (G, \cdot) is an abelian group

Example 3

- **Example 3:** Prove that the set Z of all integers with binary operation $*$ defined by $a * b = a + b + 1 \quad \forall a, b \in Z$, is an abelian group.
- **Solution:** Sum of two integers is again an integer; therefore $a + b \in Z \quad \forall a, b \in Z$

$$\Rightarrow a + b + 1 \in Z \quad \forall a, b \in Z$$

$\Rightarrow Z$ is closed with respect to $*$

Associative law for all $a, b, c \in Z$ we have $(a * b) * c = a * (b * c)$ as

$$\begin{aligned}(a * b) * c &= (a + b + 1) * c \\&= a + b + 1 + c + 1 \\&= a + b + c + 2\end{aligned}$$

also

$$\begin{aligned}a * (b * c) &= a * (b + c + 1) \\&= a + b + c + 1 + 1 \\&= a + b + c + 2\end{aligned}$$

Hence $(a * b) * c = a * (b * c) \in Z$.

Sub-Group

- **Definition:** Let $(G, *)$ be a group and H , be a non-empty subset of G . If $(H, *)$ is itself is a group, then $(H, *)$ is called sub-group of $(G, *)$.
- **Example 1:** Let $a = \{1, -1, i, -i\}$ and $H = \{1, -1\}$ G and H are groups with respect to the binary operation, multiplication.
 - H is a subset of G , therefore (H, X) is a sub-group (G, X) .
- **Example 2:** Consider $(Z_6, +_6)$, the group of integers modulo 6.
 - $H = \{0, 2, 4\}$ is a subset of Z_6 and $\{H, +_6\}$ is a group.
 - $\therefore \{H, +_6\}$ is a sub-group.

Ring

- **Definition:** An algebraic system $(R, +, \cdot)$ is called a ring if the binary operations ' $+$ ' and ' \cdot ' $\in R$ satisfy the following properties:

1. $(R, +)$ is an abelian group.
2. (R, \cdot) is a semi-group.
3. The operation ' \cdot ' is distributive over $+$,
that is for any $a, b, c \in R$,

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ and}$$

$$(b + c) \cdot a = b \cdot a + c \cdot a$$

Example

- **Example 1:** The set of integers \mathbb{Z} , with respect to the operations $+$ and \times is a ring.
- **Example 2:** The set of all matrices of the form

$$\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$$

where, a and b being real numbers,

with matrix addition and matrix multiplication is a ring.

Resource

- Discrete mathematics structures – G. Shanakr Rao - 2 Ed