

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

Today is Tuesday.

Non- $x + y > 0$

examples:

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

They are true for some values of x and y

but are false for some other values of x

and y

Logic Operators

Logic operators are used to construct new statements from old statements.

There are three main logic operators, NOT, AND, OR.

$\wedge ::= \text{AND}$

$\vee ::= \text{OR}$

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

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

Logic Operators

Logic operators are used to construct new statements from old statements.

There are three main logic operators, NOT, AND, OR.

$\neg ::= \text{NOT}$ $\neg P$ is true if and only if P is false

P	$\neg P$
T	F
F	T

Compound Statement

p = “it is hot”

q = “it is sunny”

It is hot and sunny

$$p \wedge q$$

It is not hot but sunny

$$\neg p \wedge q$$

It is neither hot nor sunny

$$\neg p \wedge \neg q$$

We can also define logic operators on three or more statements, e.g. OR(I

More Logical Operators

We can define more logical operators as we need.

coffee “or” tea

majority

\oplus exclusive-or

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

P	Q	R	M(P,Q,R)
T	T	T	T
T	T	F	T
T	F	T	T
T	F	F	F
F	T	T	T
F	T	F	F
F	F	T	F
F	F	F	F

Logical Form

- Truth table for $(\sim p \wedge q) \vee (q \wedge \sim r)$
- Two statements are called logically equivalent if and only if (iff) they have identical truth tables
- Double negation
- Non-equivalence: $\sim(p \vee q)$ vs $\sim p \vee \sim q$
- De Morgan's Laws:
 - The negation of an AND statement is logically equivalent to the OR statement in which component is negated
 - The negation of an OR statement is logically equivalent to the AND statement in which each component is negated

- ⊙ Applying De-Morgan's Laws:
 - Write negation for
 - The bus was late or Tom's watch was slow
 - $-1 < x \leq 4$
- ⊙ Tautology is a statement that is always true regardless of the truth values of the individual logical variables
- ⊙ Contradiction is a statement that is always false regardless of the truth values of the individual logical variables

Exclusive-Or

Is there a more systematic way to construct such a formula?

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

Idea 1: Look at the true rows

Want the formula to be true exactly when the input belongs to a “true” row.

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

The input is the second row exactly if this sub-formula is satisfied

And the formula is true exactly when the input is the second row **or** the th

Exclusive-Or

Is there a more systematic way to construct such a formula?

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

Idea 2: Look at the false rows

Want the formula to be true exactly when the input does **not** belong to a “false” row.

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

The input is the first row exactly if this sub-formula is satisfied

And the formula is true exactly when the input is **not** in the 1st row **and** the

DeMorgan's Laws

Logical equivalence: Two statements have the same truth table

Statement: Tom is in the football team and the basketball team.

Negation: Tom is not in the football team or not in the basketball team.

De Morgan's Law $\neg(p \wedge q) \equiv \neg p \vee \neg q$

Why the negation of the above statement is not the following

“Tom is not in the football team and not in the basketball team”?

The definition of the negation is that exactly one of P or ¬P is true, but

could be the case that both the above statement and the original statement

are false (e.g. Tom is in the football team but not in the basketball team).

Conditional Statements

- ⊙ If something, then something: $p \rightarrow q$, p is called the hypothesis and q is called the conclusion
- ⊙ The only combination of circumstances in which a conditional sentence is false is when the hypothesis is true and the conclusion is false
- ⊙ A conditional statements is called vacuously true or true by default when its hypothesis is false
- ⊙ Among \wedge , \vee , \sim and \rightarrow operations, \rightarrow has the lowest priority

Logical Equivalence

- Commutative laws: $p \wedge q = q \wedge p$, $p \vee q = q \vee p$
- Associative laws: $(p \wedge q) \wedge r = p \wedge (q \wedge r)$, $(p \vee q) \vee r = p \vee (q \vee r)$
- Distributive laws: $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$
 $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$
- Identity laws: $p \wedge t = p$, $p \vee c = p$
- Negation laws: $p \vee \sim p = t$, $p \wedge \sim p = c$
- Double negative law: $\sim(\sim p) = p$
- Idempotent laws: $p \wedge p = p$, $p \vee p = p$
- De Morgan's laws: $\sim(p \wedge q) = \sim p \vee \sim q$, $\sim(p \vee q) = \sim p \wedge \sim q$
- Universal bound laws: $p \vee t = t$, $p \wedge c = c$
- Absorption laws: $p \vee (p \wedge q) = p$, $p \wedge (p \vee q) = p$
- Negation of t and c: $\sim t = c$, $\sim c = t$

Conditional Statements

- Contrapositive $p \rightarrow q$ is another conditional statement $\sim q \rightarrow \sim p$
- A conditional statement is equivalent to its contrapositive
- The converse of $p \rightarrow q$ is $q \rightarrow p$
- The inverse of $p \rightarrow q$ is $\sim p \rightarrow \sim q$
- Conditional statement and its converse are not equivalent
- Conditional statement and its inverse are not equivalent

Conditional Statements

- The converse and the inverse of a conditional statement are equivalent to each other
- p only if q means $\sim q \rightarrow \sim p$, or $p \rightarrow q$
- Biconditional of p and q means “ p if and only if q ” and is denoted as $p \leftrightarrow q$
- r is a sufficient condition for s means “if r then s ”
- r is a necessary condition for s means “if not r then not s ”

Arguments

- An argument is a sequence of statements. All statements except the final one are called premises (or assumptions or hypotheses). The final statement is called the conclusion.
- An argument is considered valid if from the truth of all premises, the conclusion must also be true.
- The conclusion is said to be inferred or deduced from the truth of the premises

Contradiction

- ◉ Contradiction rule: if one can show that the supposition that a statement p is false leads to a contradiction, then p is true.
- ◉ Knight is a person who always says truth, knave is a person who always lies:
 - A says: B is a knight
 - B says: A and I are of opposite typesWhat are A and B?

DeMorgan's Laws

Logical equivalence: Two statements have the same truth table

Statement: The number 783477841 is divisible by 7 or 11.

Negation: The number 783477841 is not divisible by 7 and not divisible by 11.

De Morgan's Law $\neg(p \vee q) \equiv \neg p \wedge \neg q$

Again, the negation of the above statement is not

“The number 783477841 is not divisible by 7 or not divisible by 11”

In either case, we “flip” the inside operator from OR to AND or from AND to OR.

Simplifying Statement

We can use logical rules to simplify a logical formula.

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

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

DeMorgan

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

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

Distributive law

$$\equiv p \vee \text{False}$$

$$\equiv p$$

The DeMorgan's Law allows us to always “move the NOT inside

(Optional) See textbook for more identities.

Tautology, Contradiction

A tautology is a statement that is always true.

$$p \vee \neg p$$

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

A contradiction is a statement that is always false (negation of a tautology).

$$p \wedge \neg p$$

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

In general it is “difficult” to tell whether a statement is a contradiction.

It is one of the most important problems in CS – the satisfiability problem.

Logic Operator

$\rightarrow ::=$ IMPLIES

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

Convention: if we don't say anything wrong, then it is not false, and thus true.

Make sure you understand the definition of IF.

The IF operation is very important in mathematical proofs.

Logical Equivalence

$$p \rightarrow q \equiv ?$$

If you see a question in the above form, there are usually 3 ways to deal with it.

- (1) Truth table
- (2) Use logical rules
- (3) Intuition

If-Then as Or

$$p \rightarrow q \equiv ?$$

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Idea 2: Look at the false rows,
negate and take the “and”.

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

$$\equiv \neg P \vee Q$$

- If you don't give me all your money, then I will kill you.
- Either you give me all your money or I will kill you (or both).
- If you talk to her, then you can never talk to me.
- Either you don't talk to her or you can never talk to me (or both).

Negation of If-Then

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

- If you eat an apple everyday, then you have no toothache.
- You eat an apple everyday but you have toothache.
- If my computer is not working, then I cannot finish my homework.
- My computer is not working but I can finish my homework.

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

$$\equiv \neg(\neg P \vee Q)$$

previous slide

$$\equiv \neg\neg P \wedge \neg Q$$

DeMorgan

$$\equiv P \wedge \neg Q$$

Contrapositive

The **contrapositive** of “if p then q ” is “if $\sim q$ then $\sim p$ ”.

Statement: If you are a CS year 1 student,
then you are taking CSC 2110.

Contrapositive: If you are not taking CSC 2110,
then you are not a CS year 1 student.

Statement: If you drive, then you don't drink.

Contrapositive: If you drink, then you don't drive.

Fact: A conditional statement is logically equivalent to its contrapositive.

Proofs

Statement: If P, then Q

Contrapositive: $\neg Q$, then $\neg P$.

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

In words, the only way the above statements are false is when P true and Q

Contrapositive

Statement: If P, then Q

Contrapositive: $\neg Q$, then $\neg P$.

Or we can see it using logical rules:

$$P \rightarrow Q \equiv \neg P \vee Q \equiv Q \vee \neg P \equiv \neg Q \rightarrow \neg P$$

Contrapositive is useful in mathematical proofs, e.g. to prove

Statement: If x^2 is an even number, then x is an even number.

You could instead prove:

Contrapositive: If x is an odd number, then x^2 is an odd number.

This is equivalent and is easier to prove.

Definitions

- Tautology – a logical expression that is true for all variable assignments.
- Contradiction – a logical expression that is false for all variable assignments.
- Contingent – a logical expression that is neither a tautology nor a contradiction.

Normal Forms

- Normal forms are standard forms, sometimes called canonical or accepted forms.
- A logical expression is said to be in disjunctive normal form (DNF) if it is written as a disjunction, in which all *terms* are conjunctions of *literals*.
- Similarly, a logical expression is said to be in conjunctive normal form (CNF) if it is written as a conjunction of disjunctions of literals.

DNF and CNF

Disjunctive Normal Form (DNF)

$$(\dots \wedge \dots \wedge \dots) \vee (\dots \wedge \dots \wedge \dots) \vee \dots \vee (\dots \wedge \dots)$$

Term

Literal, i.e. P or $\neg P$

Examples: $(P \wedge Q) \vee (P \wedge \neg Q)$

$$P \vee (Q \wedge R)$$

Conjunctive Normal Form (CNF)

$$(\dots \vee \dots \vee \dots) \wedge (\dots \vee \dots \vee \dots) \wedge \dots \wedge (\dots \vee \dots)$$

Examples: $(P \vee Q) \wedge (P \vee \neg Q)$

$$P \wedge (Q \vee R)$$

Converting Expressions to DNF or CNF

The following procedure converts an expression to DNF or CNF:

1. Remove all \Rightarrow and \Leftrightarrow .
2. Move \neg inside. (Use De Morgan's law.)
3. Use distributive laws to get proper form.

Simplify as you go. (e.g. double-neg., idemp., comm., assoc.)

CNF Conversion Example

$(\dots \vee \dots \vee \dots) \wedge (\dots \vee \dots \vee \dots) \wedge \dots \wedge (\dots \vee \dots)$

$$\neg((\neg P \vee Q) \wedge R \wedge (P \Rightarrow Q))$$

$$\equiv \neg((\neg P \vee Q) \wedge R \wedge (\neg P \vee Q))$$

impl.

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

deM.

$$\equiv (\neg\neg P \wedge \neg Q) \vee \neg R \vee (\neg\neg P \wedge \neg Q)$$

deM.

$$\equiv (P \wedge \neg Q) \vee \neg R \vee (P \wedge \neg Q)$$

double neg.

$$\text{(DNF)} \equiv ((P \vee \neg R) \wedge (\neg Q \vee \neg R)) \vee (P \wedge \neg Q)$$

distr.

$$\equiv ((P \vee \neg R) \vee (P \wedge \neg Q)) \wedge$$

distr.

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

$$\equiv (((P \vee \neg R) \vee P) \wedge ((P \vee \neg R) \vee \neg Q)) \wedge \text{distr.}$$

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

$$\equiv (P \vee \neg R) \wedge (P \vee \neg R \vee \neg Q) \wedge (\neg Q \vee \neg R)$$

assoc. comm.

idemp.

CNF Conversion Example

$$(.. \vee .. \vee ..) \wedge (.. \vee .. \vee ..) \wedge \dots \wedge (.. \vee ..)$$

$$\neg((\neg P \vee Q) \wedge R \wedge (P \Rightarrow Q))$$

$$\equiv \neg((\neg P \vee Q) \wedge R \wedge (\neg P \vee Q))$$

impl.

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

deM.

$$\equiv (\neg\neg P \wedge \neg Q) \vee \neg R \vee (\neg\neg P \wedge \neg Q)$$

deM.

$$\equiv (P \wedge \neg Q) \vee \neg R \vee (P \wedge \neg Q)$$

double neg.

$$(DNF) \equiv ((P \vee \neg R) \wedge (\neg Q \vee \neg R)) \vee (P \wedge \neg Q)$$

distr.

$$\equiv ((P \vee \neg R) \vee (P \wedge \neg Q)) \wedge$$

distr.

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

$$\equiv (((P \vee \neg R) \vee (P \wedge \neg Q)) \wedge ((\neg Q \vee \neg R) \vee (P \wedge \neg Q))) \wedge$$

distr.

CNF

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

assoc. comm.

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

Using the commutative and idempotent laws on the previous step and then the distributive law, we obtain this formula as the conjunctive normal form.

CNF Conversion Example

$$\neg((\neg P \vee Q) \wedge R \wedge (P \Rightarrow Q))$$

$$\equiv \neg((\neg P \vee Q) \wedge R \wedge (\neg P \vee Q))$$

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

$$\equiv (\neg\neg P \wedge \neg Q) \vee \neg R \vee (\neg\neg P \wedge \neg Q)$$

$$\equiv (P \wedge \neg Q) \vee \neg R \vee (P \wedge \neg Q)$$

$$\text{(DNF)} \equiv ((P \vee \neg R) \wedge (\neg Q \vee \neg R)) \vee (P \wedge \neg Q)$$

$$\equiv ((P \vee \neg R) \vee (P \wedge \neg Q)) \wedge ((\neg Q \vee \neg R) \vee (P \wedge \neg Q))$$

$$\equiv (((P \vee \neg R) \vee P) \wedge ((P \vee \neg R) \vee (P \wedge \neg Q))) \wedge (((\neg Q \vee \neg R) \vee P) \wedge ((\neg Q \vee \neg R) \vee \neg Q))$$

$$\equiv (P \vee \neg R) \wedge (P \vee \neg R \vee \neg Q) \wedge (\neg Q \vee \neg R)$$

$$\equiv (P \vee \neg R) \wedge (P \vee \neg R \vee \neg Q) \wedge (\neg Q \vee \neg R)$$

$$\equiv (P \vee \neg R) \wedge (P \vee \neg R \vee \neg Q) \wedge (\neg Q \vee \neg R)$$

idemp.

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

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

$$\equiv (P \vee \neg R) \wedge (P \vee \neg R \vee \neg Q)$$

$$\wedge (F \vee \neg Q \vee \neg R) \text{ - ident.}$$

$$\equiv (P \vee \neg R) \wedge ((P \wedge F) \vee (\neg Q \vee \neg R)) \text{ - comm., distr.}$$

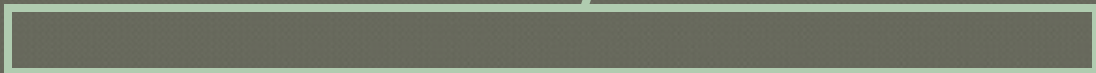
$$\equiv (P \vee \neg R) \wedge (F \vee (\neg Q \vee \neg R)) \text{ - dominat.}$$

$$\equiv (P \vee \neg R) \wedge (\neg Q \vee \neg R) \text{ - ident.}$$

$$\equiv (P \vee \neg R) \wedge (\neg Q \vee \neg R) \text{ - ident.}$$

$$\equiv (P \vee \neg R) \wedge (\neg Q \vee \neg R) \text{ - ident.}$$

assoc. comm.



: Predicates

- ✦ Predicate logic
- ✦ Free and bound variables
- ✦ Rules of Inference
- ✦ Consistency
- ✦ Proof of Contradiction

Quantifiers and Predicates

✦ Universal quantifier : The quantifier ‘ all ’ is called the Universal quantifier, and we shall denote it by $\forall x$ (or (x)), which is an inverted A followed by the variable x.

$\forall x$: for all x (for every x (or) for each x)

✦ Existential quantifier : The quantifier ‘ some ’ is called the Existential quantifier, and we shall denote it by $\exists x$, which is a reversed E followed by the variable x.

$\exists x$: for some x (There exists an x such that or There is at least one x such that)

✦ Consider the statement, ‘ John is a Politician ’

Here, ‘ John ’ is the subject and ‘ is a Politician ’ is the predicate

Denote the predicate, ‘ is a Politician ’ symbolically by the predicate letter P, and the subject ‘ John ’ by j .

Predicates (Contd.,)

✦ The statement ‘John is a Politician’ can be written as $P(j)$

$P(j)$: John is a Politician

✦ If x is any person, then

$P(x)$: x is a politician

✦ In general, any statement of the type “ x is Q ” is denoted by $Q(x)$.

✦ Let $S(x)$: x is a scientist. (Here, S denote the predicate ‘is a scientist’).

✦ $\neg P(x)$: x is not a politician

✦ $P(x) \wedge S(x)$: x is a politician and x is a scientist.

✦ $P(x) \vee S(x)$: Either x is a politician or x is a scientist.


✦ $P(x) \rightarrow S(y)$: If x is a politician then y is a scientist.

✦ $\forall x \{P(x)\}$: All are politicians

Sentences with Multiple quantifiers


- ✦ In general, $P(x,y)$ is any predicate involving the two variables x and y .
- ✦ Let $L(x,y)$: x likes y (Here, L denotes the predicate 'Likes', x and y are any two persons), then the following possibilities exist:
 - ✦ $(\forall x) (\forall y) L(x,y)$: Every body likes every body.
 - ✦ $(\forall x) (\exists y) L(x,y)$: Every body likes some body.
 - ✦ $(\exists x) (\forall y) L(x,y)$: Some body likes every body.
 - ✦ $(\exists x) (\exists y) L(x,y)$: Some body likes Some body.
 - ✦ $(\forall y) (\forall x) L(x,y)$: Every body was liked by every body.
 - ✦ $(\exists y) (\forall x) L(x,y)$: There is some body who is liked by every body.
 - ✦ $(\forall y) (\exists x) L(x,y)$: Every body is liked by some one.
 - ✦ $(\exists y) (\exists x) L(x,y)$: Some body was liked by some body.

Rules of Inference

 **Universal specification** : If a statement of the form $(\forall x) P(x)$ is assumed to be true then the universal quantifier can be dropped to obtain $P(c)$ is true for an arbitrary object c in the universe. This rule may be represented as

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


$$\forall P(c) \text{ for all } c.$$

 **Universal generalization**: If a statement $P(c)$ is true for each element c of the universe, then the universal quantifier may be prefixed to obtain $(\forall x) P(x)$. In symbols, this rule is

$$\underline{P(c) \text{ for all } c}$$


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

Rules of Inference

 **Existential specification:** If $(\exists x) P(x)$ is assumed to be true, then there is an element c in the universe such that $P(c)$ is true. This rule takes the form

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

$$\exists P(c) \text{ for some } c$$

 **Existential generalization:** If $P(c)$ is true for some element c in the universe, then $\exists x, P(x)$ is true. In symbols, we have

$$\underline{P(c) \text{ for some } c}$$

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

Free and Bound variables

✦ Given a formula containing a part of the form $(\forall x) P(x)$ or $(\exists x) P(x)$, such a part is called an x-bound part of the formula. Further $P(x)$ is the scope of the quantifier in both the formulas.

✦ Any occurrence of x , in an x-bound part of the formula is called a bound occurrence of x , while any variable that is not a bound occurrence is called a free occurrence

✦ Ex: consider, $(\forall x) P(x,y)$

Here, the scope of the universal quantifier is $P(x,y)$, x is a bound variable and y is a free variable.

✦ Ex: Consider the formula, $(\forall x) (P(x) \wedge Q(x))$

Here, Scope of the quantifier is $P(x) \wedge Q(x)$.

Both the occurrences of x are bound.

Free and Bound variables (Contd.,)

✦ Ex: $(\forall x) \{P(x) \wedge (\forall y) R(x,y)\}$

Here, the scope of $\forall x$ is $P(x) \wedge (\forall y) R(x,y)$

and the scope of $\forall y$ is $R(x,y)$

All occurrences of x and y are bound occurrences.

✦ In the bound occurrence of a variable, the letter which is used to represent the variable is a dummy variable.

The formula $(\forall x) \{P(x)\}$ is same as $(\forall y) \{P(y)\}$

The formula, $(\forall y) R(x,y)$ is same as $(\forall z) R(x,z)$.

✦ Generally speaking, in order to draw conclusions from quantified premises, we need to remove quantifiers properly, argue with the resulting propositions, and then properly prefix the correct quantifiers.

Examples

✦ Ex: Let $P(x)$: x is a person

$F(x,y)$: x is the father of y

$M(x,y)$: x is the mother of y

Write the predicate “ x is the father of the mother of y ” in symbolic form.

✦ Solution: In order to symbolize the predicate, let us assume a person called z as the mother of y.

Now, x is the father of z and z is the mother of y .

We symbolize the predicate as

$$(\exists z) \{ P(z) \wedge F(x, z) \wedge M(z, y) \}$$

Ex: Symbolize the expression “All the world loves a lover”

✦ Solution: First, let us note that the quotation really means that every body loves a lover.

Now let

$P(x)$: x is a person

$L(x)$: x is a lover

$Q(x, y)$: x loves y

The required expression is

$$(\forall x) [P(x) \supset (\exists y)\{P(y) \supset L(y) \supset Q(x, y)\}]$$

Ex: prove the following argument

$$(1) (\forall x) \{P(x) \supset Q(x)\}$$

$$(2) \underline{(\forall x) [\{\neg P(x) \supset Q(x)\} \supset R(x)]}$$

$$\supset (\forall x) \{\neg R(x) \supset P(x)\}$$

✦ Proof: From (1), By the rule of US, we have

$$P(c) \supset Q(c) \dots(3)$$

From (2), By the rule of US, we have

$$\{\neg P(c) \supset Q(c)\} \supset R(c) \dots(4)$$

From (4), By contra positive equivalence, we have

$$\neg R(c) \supset \{P(c) \supset \neg Q(c)\} \dots(5)$$

Let $\neg R(c) \dots(6)$ (Additional premise)

From (5) and (6), By the rule of modus ponens, we have

$$P(c) \supset \neg Q(c) \dots(7)$$

From (3) and (7), we have

$$\{P(c) \supset Q(c)\} \supset \{P(c) \supset \neg Q(c)\}$$

Contd.,

$\square P(c) \square \{Q(c) \square \square Q(c)\}$

$\square P(c) \square F$

$\square P(c)$

Now, By CP rule,

$\square R(c) \square P(c) \dots(8)$ follows

From (8), By the rule of UG, we have

$(\square x) \{ \square R(x) \square P(x) \}$

Hence, the given argument is valid.

Automatic Theorem proving

✦ String of Formulas: A string of formulas is defined as follows.

A) Any formula is a string of formulas

B) If ϕ and ψ are strings of formulas, then

ϕ, ψ and ϕ, ψ are strings of formulas.

C) Only those strings which are obtained by steps (A) and (B) are strings of formulas, with the exception of empty string which is also a string of formulas.

✦ Sequents : If ϕ and ψ are strings of formulas, then $\phi^S \psi$ is called a sequent in which ϕ is called antecedent and ψ is called consequent.

Sequents (Contd.,)

✦ A sequent $\Gamma \overset{S}{\vdash} \Delta$ is true if and only if either at least one of the formulas of the antecedent is false or at least one of the formulas of the consequent is true.

✦ Thus

$A, B, C \overset{S}{\vdash} D, E, F$ is true iff $(A \wedge B \wedge C) \wedge (D \wedge E \wedge F)$ is true .

✦ $\Gamma \overset{S}{\vdash} \Delta$ means that $\Gamma \overset{S}{\vdash} \Delta$ is true.

✦ The empty antecedent is interpreted as ‘true’ or T

✦ The empty consequent is interpreted as ‘false’ or F

✦ Axiom schema: If Γ and Δ are strings of formulas such that every formula in both Γ and Δ is a variable only, then the sequent $\Gamma \overset{S}{\vdash} \Delta$ is an axiom iff Γ and Δ have at least one variable in common.

Axioms –theorems -Rules

✦ Ex: $A, B, C \vdash P, B, R$ is an axiom.

If $\Gamma \vdash \Delta$ is an axiom, then $\Gamma \vdash \Delta$.

✦ Theorem: The following sequents are theorems of our system.

a) Every axiom is a theorem .

b) If a sequent $\Gamma \vdash \Delta$ is a theorem and a sequent $\Gamma' \vdash \Delta'$ results from $\Gamma \vdash \Delta$ through the use of one of the 10 rules of the system which are given below, then $\Gamma' \vdash \Delta'$ is a theorem.

c) Sequents obtained by (a) and (b) are the only theorems.

✦ Rules: The following rules are used to combine formulas within strings by introducing connectives. Corresponding to each of the connectives there are two rules, one for introducing the connective in the antecedent and the other for its introduction in the consequent.

Rules for Automatic Theorem proving

☀ Antecedent rules:

☀ Rule □□ : If □, □^S X, □ then □, □X, □^S □□

☀ Rule □□ : If X, Y, □, □^S □□ then □, X□Y, □^S □□

☀ Rule □□ : If X, □, □^S □□ and Y, □, □^S □□,
then □, X□Y, □^S □□

☀ Rule □□ : If Y, □, □^S □□ and □, □^S X, □
then □, X□Y, □^S □□

☀ Rule □□ : If X, Y, □, □^S □□ and □, □^S X, Y, □
then □, X□Y, □^S □□

Rules for Automatic Theorem proving (contd.,)

✦ Consequent rules:

✦ Rule □□ : If $X, \square \text{ S } \square, \square$ then $\square \text{ S } \square, \square X, \square$

✦ Rule □□ : If $\square \text{ S } X, \square, \square$ and $\square \text{ S } \square Y, \square, \square$
then $\square \text{ S } \square, X \square Y, \square$

✦ Rule □□ : If $\square \text{ S } X, Y, \square, \square$ then $\square \text{ S } \square, X \square Y, \square$

✦ Rule □□ : If $X, \square \text{ S } Y, \square, \square$ and $\square \text{ S } \square, X \square Y, \square$

✦ Rule □□ : If $X, \square \text{ S } Y, \square, \square$ and $Y, \square \text{ S } X, \square, \square$
then $\square \text{ S } \square, X \square Y, \square$

Examples

✦ Ex: Using Automatic theorem proving, Show that $P \rightarrow Q$ follows from P.

✦ Solution: we need to show that

(1) $\vdash P \rightarrow (P \rightarrow Q)$

(1) if (2) $\vdash P \rightarrow (P \rightarrow Q)$ (By the rule, \rightarrow I)

(2) if (3) $\vdash P, Q$ (By the rule, \rightarrow I)

Now, (3) is an axiom

Hence, the theorem (1) follows.

Ex: Using Automatic theorem proving,
Show that P does not follow from $P \sqsupset Q$.

✦ Solution: Assume

✦ (1) $\neg (P \sqsupset Q) \sqsupset P$

(1) if (2) $(P \sqsupset Q) \sqsupset P$ (By the rule, $\neg \neg$)

(2) if (3) $P \sqsupset P$ and (4) $Q \sqsupset P$ (By the rule, $\neg \neg$)

Note that (3) is an axiom, but (4) is not.

Hence, P does not follow from $P \sqsupset Q$.

Ex: Using Automatic theorem proving, prove the following

- (a) $\{P \rightarrow (\neg P \rightarrow Q)\} \rightarrow R$
 (b) $R \rightarrow \{P \rightarrow (\neg P \rightarrow Q)\}$

✦ Solution: (a) To show (1) $\vdash \{P \rightarrow (\neg P \rightarrow Q)\} \rightarrow R$

(1) if (2) $\{P \rightarrow (\neg P \rightarrow Q)\} \vdash R$ (By using the rule, \rightarrow E, twice)

(2) if (3) $\{P, \neg P, Q\} \vdash R$ (By the rule, \rightarrow I)

(3) if (4) $\{P, Q\} \vdash \{P, R\}$ (By the rule, \rightarrow I)

Now (4) is an axiom , therefore the result follows.

✦ (b) To show (1) $\vdash R \rightarrow \{P \rightarrow (\neg P \rightarrow Q)\}$

(1) if (2) $R \vdash \{P \rightarrow (\neg P \rightarrow Q)\}$ (By the rule, \rightarrow I)

(2) if (3) $R \vdash \{P, \neg P, Q\}$ (By using the rule, \rightarrow E , twice)

(3) if (4) $\{R, P\} \vdash \{P, Q\}$ (By using the rule, \rightarrow I)

Now (4) is an axiom , therefore the result follows.

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 $a \nabla R b$ to denote that $(a, b) \notin R$.

Relations

Relations

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.

Functions as Relations

You might remember that a **function** f from a set A to a set B assigns a unique element of B to each element of A .

The **graph** of f is the set of ordered pairs (a, b) such that $b = f(a)$.

Since the graph of f is a subset of $A \times B$, it is a **relation** from A to B .

Moreover, for each element a of A , there is exactly one ordered pair in the graph that has a as its first element.

Functions as Relations

Conversely, if R is a relation from A to B such that every element in A is the first element of exactly one ordered pair of R , then a function can be defined with R as its graph.

This is done by assigning to an element $a \in A$ the unique element $b \in B$ such that $(a, b) \in R$.

Relations on a Set

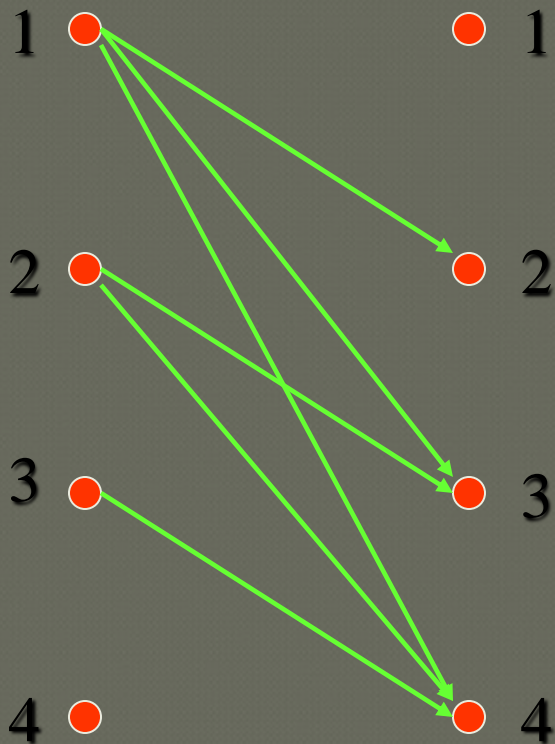
Definition: A relation on the set A is a relation from A to A .

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 $R = \{(a, b) \mid a < b\}$?

Relations on a Set

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				

Properties of Relations

We will now look at some useful ways to classify relations.

Definition: A relation R on a set A is called **reflexive** if $(a, a) \in R$ for every element $a \in A$.

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.

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

Properties of Relations

Definitions:

A relation R on a set A is called **symmetric** if $(b, a) \in R$ whenever $(a, b) \in R$ for all $a, b \in A$.

A relation R on a set A is called **antisymmetric** if $a = b$ whenever $(a, b) \in R$ and $(b, a) \in R$.

A relation R on a set A is called **asymmetric** if $(a, b) \in R$ implies that $(b, a) \notin R$ for all $a, b \in A$.

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.

Properties of Relations

Definition: A relation R on a set A is called **transitive** if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$ for $a, b, c \in A$.

Are the following relations on $\{1, 2, 3, 4\}$ transitive?

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

Yes.

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

No.

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

No.

Counting Relations

Example: How many different reflexive relations can be defined on a set A containing n elements?

Solution: Relations on R are subsets of $A \times A$, which contains n^2 elements.

Therefore, different relations on A can be generated by choosing different subsets out of these n^2 elements, so there are 2^{n^2} relations.

A **reflexive** relation, however, **must** contain the n elements (a, a) for every $a \in A$.

Consequently, we can only choose among $n^2 - n = n(n - 1)$ elements to generate reflexive relations, so there are $2^{n(n - 1)}$ of them.

Combining Relations

Relations are sets, and therefore, we can apply the usual **set operations** to them.

If we have two relations R_1 and R_2 , and both of them are from a set A to a set B , then we can combine them to $R_1 \cup R_2$, $R_1 \cap R_2$, or $R_1 - R_2$.

In each case, the result will be **another relation from A to B** .

Combining Relations

... and there is another important way to combine relations.

Definition: 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 **$S \circ R$** .

In other words, if relation R contains a pair (a, b) and relation S contains a pair (b, c) , then $S \circ R$ contains a pair (a, c) .

Combining Relations

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

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

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

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

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

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

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 $S \circ D = \{(a, b) \mid a + b > 5\}$.

Combining Relations

We already know that **functions** are just **special cases** of **relations** (namely those that map each element in the domain onto exactly one element in the codomain).

If we formally convert two functions into relations, that is, write them down as sets of ordered pairs, the composite of these relations will be exactly the same as the composite of the functions (as defined earlier).

Combining Relations

Definition: Let R be a relation on the set A . The powers R^n , $n = 1, 2, 3, \dots$, are defined inductively by

$$R^1 = R$$

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

In other words:

$$R^n = R \circ R \circ \dots \circ R \quad (n \text{ times the letter } R)$$

Combining Relations

Theorem: The relation R on a set A is transitive if and only if $R^n \subseteq R$ for all positive integers n .

Remember the definition of transitivity:

Definition: A relation R on a set A is called transitive if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$ for $a, b, c \in A$.

The composite of R with itself contains exactly these pairs (a, c) .

Therefore, for a transitive relation R , $R \circ R$ does not contain any pairs that are not in R , so $R \circ R \subseteq R$.

Since $R \circ R$ does not introduce any pairs that are not already in R , it must also be true that $(R \circ R) \circ R \subseteq R$, and so on, so that $R^n \subseteq R$.

n-ary Relations

In order to study an interesting application of relations, namely **databases**, we first need to generalize the concept of binary relations to **n-ary relations**.

Definition: Let A_1, A_2, \dots, A_n be sets. An **n-ary relation** on these sets is a subset of $A_1 \times A_2 \times \dots \times A_n$. The sets A_1, A_2, \dots, A_n are called the **domains** of the relation, and n is called its **degree**.

n-ary Relations

Example:

Let $R = \{(a, b, c) \mid a = 2b \wedge b = 2c \text{ with } a, b, c \in \mathbf{N}\}$

What is the degree of R?

The degree of R is 3, so its elements are triples.

What are its domains?

Its domains are all equal to the set of integers.

Is (2, 4, 8) in R?

No.

Is (4, 2, 1) in R?

Yes.

Representing Relations

We already know different ways of representing relations. We will now take a closer look at two ways of representation: **Zero-one matrices** and **directed graphs**.

If R is a relation from $A = \{a_1, a_2, \dots, a_m\}$ to $B = \{b_1, b_2, \dots, b_n\}$, then R can be represented by the zero-one matrix $M_R = [m_{ij}]$ with

$m_{ij} = 1$, if $(a_i, b_j) \in R$, and

$m_{ij} = 0$, if $(a_i, b_j) \notin R$.

Note that for creating this matrix we first need to list the elements in A and B in a **particular, but arbitrary order**.

Representing Relations

Example: How can we represent the relation $R = \{(2, 1), (3, 1), (3, 2)\}$ as a zero-one matrix?

Solution: The matrix M_R is given by

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

Representing Relations

What do we know about the matrices representing **symmetric relations**?

These matrices are symmetric, that is, $M_R = (M_R)^t$.

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

symmetric matrix,
symmetric relation.

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

non-symmetric matrix,
non-symmetric relation.

Representing Relations

The Boolean operations **join** and **meet** (you remember?) can be used to determine the matrices representing the **union** and the **intersection** of two relations, respectively.

To obtain the **join** of two zero-one matrices, we apply the Boolean “or” function to all corresponding elements in the matrices.

To obtain the **meet** of two zero-one matrices, we apply the Boolean “and” function to all corresponding elements in the matrices.

Representing Relations

Example: Let the relations R and S be represented by the matrices

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

What are the matrices representing $R \cup S$ and $R \cap S$?

Solution: These matrices are given by

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

Representing Relations Using Matrices

Example: How can we represent the relation $R = \{(2, 1), (3, 1), (3, 2)\}$ as a zero-one matrix?

Solution: The matrix M_R is given by

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

Representing Relations Using Matrices

Example: Let the relations R and S be represented by the matrices

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

What are the matrices representing $R \cup S$ and $R \cap S$?

Solution: These matrices are given by

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

Representing Relations Using Matrices

Do you remember the **Boolean product** of two zero-one matrices?

Let $A = [a_{ij}]$ be an $m \times k$ zero-one matrix and
 $B = [b_{ij}]$ be a $k \times n$ zero-one matrix.

Then the **Boolean product** of A and B , denoted by $A \circ B$, is the $m \times n$ matrix with (i, j) th entry $[c_{ij}]$, where

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

$c_{ij} = 1$ if and only if at least one of the terms
 $(a_{in} \wedge b_{nj}) = 1$ for some n ; otherwise $c_{ij} = 0$.

Representing Relations Using Matrices

Let us now assume that the zero-one matrices

$M_A = [a_{ij}]$, $M_B = [b_{ij}]$ and $M_C = [c_{ij}]$ represent relations A, B, and C, respectively.

Remember: For $M_C = M_A \circ M_B$ we have:

$c_{ij} = 1$ if and only if at least one of the terms $(a_{in} \wedge b_{nj}) = 1$ for some n ; otherwise $c_{ij} = 0$.

In terms of the **relations**, this means that C contains a pair (x_i, z_j) if and only if there is an element y_n such that (x_i, y_n) is in relation A and (y_n, z_j) is in relation B.

Therefore, $C = B \circ A$ (**composite** of A and B).

Representing Relations Using Matrices

This gives us the following rule:

$$M_{B \circ A} = M_A \circ M_B$$

In other words, the matrix representing the **composite** of relations A and B is the **Boolean product** of the matrices representing A and B.

Analogously, we can find matrices representing the **powers of relations**:

$$M_{R^n} = M_R^{[n]} \quad (\text{n-th Boolean power}).$$

Representing Relations Using Matrices

Example: Find the matrix representing R^2 , where the matrix representing R is given by

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

Solution: The matrix for R^2 is given by

$$M_{R^2} = M_R^{[2]} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

Representing Relations Using Digraphs

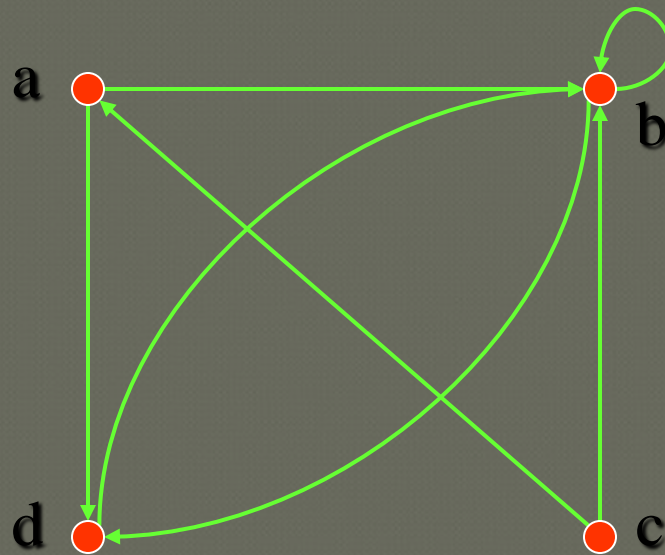
Definition: A **directed graph**, or **digraph**, consists of a set V of **vertices** (or **nodes**) together with a set E of ordered pairs of elements of V called **edges** (or **arcs**).

The vertex a is called the **initial vertex** of the edge (a, b) , and the vertex b is called the **terminal vertex** of this edge.

We can use arrows to display graphs.

Representing Relations Using Digraphs

Example: Display the digraph with $V = \{a, b, c, d\}$,
 $E = \{(a, b), (a, d), (b, b), (b, d), (c, a), (c, b), (d, b)\}$.



An edge of the form (b, b) is called a **loop**.

Representing Relations Using Digraphs

Obviously, we can represent any relation R on a set A by the digraph with A as its vertices and all pairs $(a, b) \in R$ as its edges.

Vice versa, any digraph with vertices V and edges E can be represented by a relation on V containing all the pairs in E .

This **one-to-one correspondence** between relations and digraphs means that any statement about relations also applies to digraphs, and vice versa.

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**.

Equivalence Relations

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.

Equivalence Relations

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.

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.

Equivalence Classes

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.

Equivalence Classes

Theorem: Let R be an equivalence relation on a set A . The following statements are equivalent:

- ⊙ aRb
- ⊙ $[a] = [b]$
- ⊙ $[a] \cap [b] \neq \emptyset$

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 $i \neq j$
- ⊙ $\bigcup_{i \in I} A_i = S$

Equivalence Classes

Theorem: Let R be an equivalence relation on a set S . Then the **equivalence classes** of R form a **partition** of S . Conversely, given a partition $\{A_i \mid i \in I\}$ of the set S , there is an equivalence relation R that has the sets $A_i, i \in I$, as its equivalence classes.

Equivalence Classes

Example: Let us assume that Frank, Suzanne and George live in Boston, Stephanie and Max live in Lübeck, and Jennifer lives in Sydney.

Let R be the **equivalence relation** $\{(a, b) \mid a \text{ and } b \text{ live in the same city}\}$ on the set $P = \{\text{Frank, Suzanne, George, Stephanie, Max, Jennifer}\}$.

Then $R = \{(\text{Frank, Frank}), (\text{Frank, Suzanne}), (\text{Frank, George}), (\text{Suzanne, Frank}), (\text{Suzanne, Suzanne}), (\text{Suzanne, George}), (\text{George, Frank}), (\text{George, Suzanne}), (\text{George, George}), (\text{Stephanie, Stephanie}), (\text{Stephanie, Max}), (\text{Max, Stephanie}), (\text{Max, Max}), (\text{Jennifer, Jennifer})\}$.

Equivalence Classes

Then the **equivalence classes** of R are:

$\{\{\text{Frank, Suzanne, George}\}, \{\text{Stephanie, Max}\}, \{\text{Jennifer}\}\}$.

This is a **partition** of P .

The equivalence classes of any equivalence relation R defined on a set S constitute a partition of S , because every element in S is assigned to **exactly one** of the equivalence classes.

Equivalence Classes

Another example: Let R be the relation
 $\{(a, b) \mid a \equiv b \pmod{3}\}$ on the set of integers.

Is R an equivalence relation?

Yes, R is reflexive, symmetric, and transitive.

What are the equivalence classes of R ?

$\{\dots, -6, -3, 0, 3, 6, \dots\},$
 $\{\dots, -5, -2, 1, 4, 7, \dots\},$
 $\{\dots, -4, -1, 2, 5, 8, \dots\}$

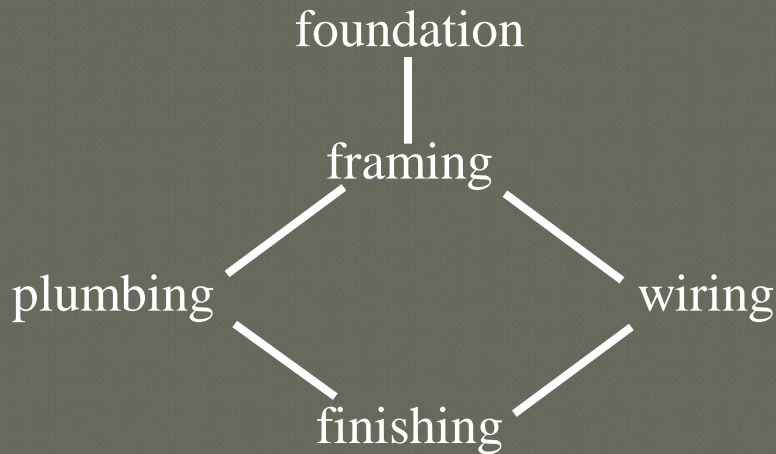
Partial Orders

Total orderings: single sequence of elements

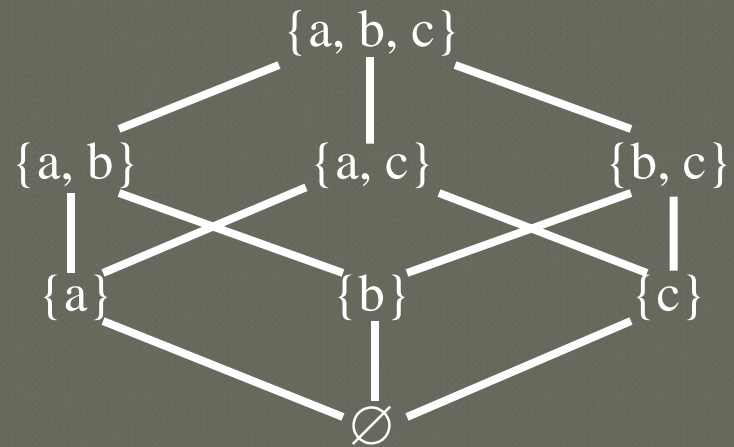
Partial orderings: some elements may come before/after others, but some need not be ordered

Examples of partial orderings:

“must be completed before”



“set inclusion, \supseteq ”



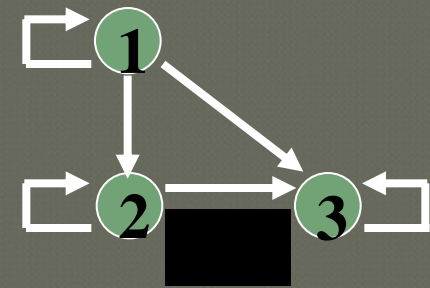
Partial Order Definitions

(Poset Definitions)

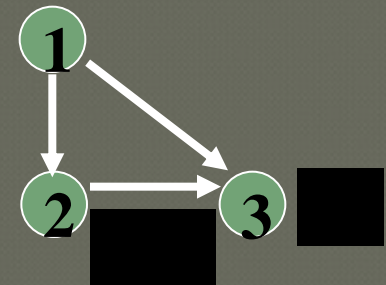
A relation $R: S \leftrightarrow S$ is called a (*weak*) *partial order* if it is reflexive, antisymmetric, and transitive.

- A relation $R: S \leftrightarrow S$ is called a *strict partial order* if it is irreflexive, antisymmetric, and transitive.

e.g. \leq on the integers



e.g. $<$ on the integers

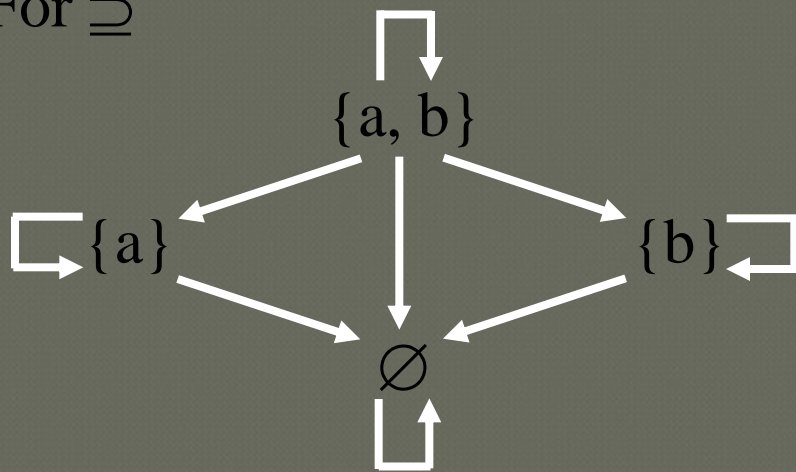


Hasse Diagrams

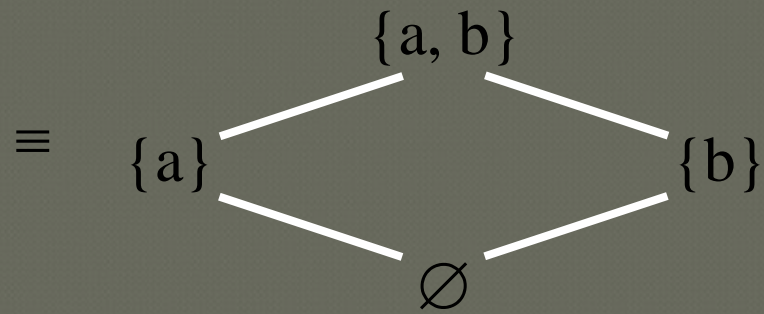
We produce Hasse Diagrams from directed graphs of relations by doing a transitive reduction plus a reflexive reduction (if weak) and (usually) dropping arrowheads (using, instead, “above” to give direction)

- 1) Transitive reduction — discard all arcs except those that “directly cover” an element.
- 2) Reflexive reduction — discard all self loops.

For \supseteq



we write:



Descending Sequence

Descending sequence: A sequence $\langle x_1, x_2, \dots, x_n \rangle$ where for $i < j$, x_i “is strictly above” x_j on a path in a Hasse diagram; x_i need not, however, be “immediately above” x_j .

Examples:

\supset	$\langle \{a,b,c\}, \{c\}, \emptyset \rangle$	descending
	$\langle \{a,b,c\}, \{b\}, \{c\}, \emptyset \rangle$	not descending
	$\langle \{a,b,c\}, \{b,c\}, \{c\}, \emptyset \rangle$	descending
\geq	$\langle 5, 4, 2 \rangle$	descending
	$\langle 3, 2, 2, 2, 1 \rangle$	not descending

Well Founded Poset

A poset is *well founded* if it has no infinite descending sequence.

Examples:

> on the integers?

$\langle 3, 2, 1, 0, -1, \dots \rangle$ not well founded

⊃ on finite sets?

$\langle \{a, b, c\}, \{c\}, \emptyset \rangle$ well founded

All finite strict posets are well founded.

⊇ on finite sets?

$\langle \{a\}, \{a\}, \{a\}, \dots \rangle$ not a descending sequence

All finite (weak) posets are well founded.

> natural numbers?

$\langle \dots, 3, 2, 1, 0 \rangle$ infinite, but well founded

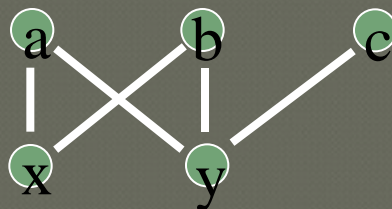
Bounds

A *least upper bound* of two elements x and y is a minimal element in the intersection of the upper bounds of x and y .

A *greatest lower bound* is a maximal element in the intersection of the lower bounds of x and y .

Examples:

- For \supseteq , $\{a, c\}$ is a least upper bound of $\{a\}$ and $\{c\}$, \emptyset is a greatest lower bound of $\{a\}$ and $\{b, c\}$, and $\{a\}$ is a least upper bound of $\{a\}$ and \emptyset .
- For the following strict poset, $\text{lub}(x, y) = \{a, b\}$, $\text{lub}(y, y) = \{a, b, c\}$, $\text{lub}(a, y) = \emptyset$, $\text{glb}(a, b) = \{x, y\}$, $\text{glb}(a, c) = \{y\}$



Groups

- ① 1. Introduction
- ② 2. Normal subgroups, quotient groups.
- ③ 3. Homomorphism.

1.Introduction

- ◎ 1.1. Binary Operations
- ◎ 1.2. Definition of Groups
- ◎ 1.3. Examples of Groups
- ◎ 1.4. Subgroups

1. Introduction

- ① 1.1. Binary Operations
- ① 1.2. Definition of Groups
- ① 1.3. Examples of Groups
- ① 1.4. Subgroups

1. Introduction

1.1. Binary Operations

A *binary operation* on a set is a rule for combining two elements of the set. More precisely, if S is a nonempty set, a binary operation on S is a mapping $f : S \times S \rightarrow S$. Thus f associates with each ordered pair (x, y) of elements of S an element $f(x, y)$ of S . It is better notation to write $x \circ y$ for $f(x, y)$, referring to \circ as the binary operation.

1.Introduction

1.2.Definition of Groups

A *group* (G, \cdot) is a set G together with a binary operation \cdot satisfying the following axioms.

- (i) The operation \cdot is associative; that is,
 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$.
- (ii) There is an *identity element* $e \in G$ such that
 $e \cdot a = a \cdot e = a$ for all $a \in G$.
- (iii) Each element $a \in G$ has an *inverse element* $a^{-1} \in G$ such that $a^{-1} \cdot a = a \cdot a^{-1} = e$.

1. Introduction

If the operation is commutative, that is,
if $a \cdot b = b \cdot a$ for all $a, b \in G$,
the group is called **commutative or
abelian, in honor of the
mathematician Niels Abel.**

1.Introduction

1.3.Examples of Groups

- **Example 1.3.1.** Let G be the set of complex numbers $\{1, -1, i, -i\}$ and let \cdot be the standard multiplication of complex numbers. Then (G, \cdot) is an abelian group. The product of any two of these elements is an element of G ; thus G is closed under the operation. Multiplication is associative and commutative in G because multiplication of complex numbers is always associative and commutative. The identity element is 1, and the inverse of each element a is the element $1/a$. Hence

$$1^{-1} = 1, (-1)^{-1} = -1, i^{-1} = -i, \text{ and } (-i)^{-1} = i.$$

1.Introduction

- **Example 1.3.2.** The set of all rational numbers, Θ , forms an abelian group $(\Theta,+)$ under addition. The identity is 0, and the inverse of each element is its negative. Similarly, $(\mathbb{Z},+)$, $(\mathbb{P},+)$, and $(\mathbb{X},+)$ are all abelian groups under addition.
- **Example 1.3.3.** If Θ^* , \mathbb{P}^* , and \mathbb{X}^* denote the set of nonzero rational, real, and complex numbers, respectively, (Θ^*, \cdot) , (\mathbb{P}^*, \cdot) , and (\mathbb{X}^*, \cdot) are all abelian groups under multiplication.

1. Introduction

- **Example 1.3.4.** A translation of the plane P^2 in the direction of the vector (a, b) is a function $f : P^2 \rightarrow P^2$ defined by $f(x, y) = (x + a, y + b)$. The composition of this translation with a translation g in the direction of (c, d) is the function

$f \circ g : P^2 \rightarrow P^2$, where

$$f \circ g(x, y) = f(g(x, y)) = f(x + c, y + d) = (x + c + a, y + d + b).$$

This is a translation in the direction of $(c + a, d + b)$. It can easily be verified that the set of all translations in P^2 forms an abelian group, under composition. The identity is the identity transformation $1_{P^2} : P^2 \rightarrow P^2$, and the inverse of the translation in the direction (a, b) is the translation in the opposite direction $(-a, -b)$.

1.Introduction

- **Example 1.3.5.** If $S(X)$ is the set of bijections from any set X to itself, then $(S(X), \circ)$ is a group under composition. This group is called the symmetric group or permutation group of X .

1. Introduction

○ **Proposition 1.3.1.** *If a , b , and c are elements of a group G , then*

(i) $(a^{-1})^{-1} = a.$

(ii) $(ab)^{-1} = b^{-1}a^{-1}.$

(iii) $ab = ac$ or $ba = ca$ implies that $b = c.$
(*cancellation law*)

1. Introduction

● 1.4. Subgroups

It often happens that some subset of a group will also form a group under the same operation. Such a group is called a *subgroup*. If (G, \cdot) is a group and H is a nonempty subset of G , then (H, \cdot) is called a *subgroup* of (G, \cdot) if the following conditions hold:

- (i) $a \cdot b \in H$ for all $a, b \in H$. (*closure*)
- (ii) $a^{-1} \in H$ for all $a \in H$. (*existence of inverses*)

1. Introduction

- Conditions (i) and (ii) are equivalent to the single condition:
(iii) $a \cdot b^{-1} \in H$ for all $a, b \in H$.

Proposition 1.4.2. *If H is a nonempty finite subset of a group G and $ab \in H$ for all $a, b \in H$, then H is a subgroup of G .*

Example 1.4.1 In the group $(\{1, -1, i, -i\}, \cdot)$, the subset $\{1, -1\}$ forms a subgroup because this subset is closed under multiplication

1. Introduction

- **Example 1.4.2** .The group Z is a subgroup of Θ , Θ is a subgroup of P , and P is a subgroup of X . (Remember that addition is the operation in all these groups.)
- However, the set $N = \{0, 1, 2, \dots\}$ of nonnegative integers is a subset of Z but not a subgroup, because the inverse of 1, namely, -1 , is not in N . This example shows that Proposition 1.4.2 is false if we drop the condition that H be finite.
- The relation of being a subgroup is transitive. In fact, for any group G , the inclusion relation between the subgroups of G is a partial order relation.

1.Introduction

- **Definition.** Let G be a group and let $a \in G$. If $a^k = 1$ for some $k \geq 1$, then the smallest such exponent $k \geq 1$ is called the *order of a* ; if no such power exists, then one says that a has *infinite order*.
- **Proposition 1.4.3 .** *Let G be a group and assume that $a \in G$ has finite order k . If $a^n = 1$, then $k \mid n$. In fact, $\{n \in \mathbb{Z} : a^n = 1\}$ is the set of all the multiples of k*

1. Introduction

- **Definition.** If G is a group and $a \in G$, write $\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{\text{all powers of } a\}$. It is easy to see that $\langle a \rangle$ is a subgroup of G . $\langle a \rangle$ is called the *cyclic subgroup* of G generated by a . A group G is called *cyclic* if there is some $a \in G$ with $G = \langle a \rangle$; in this case a is called a *generator* of G .
- **Proposition 1.4.4.** *If $G = \langle a \rangle$ is a cyclic group of order n , then a^k is a generator of G if and only if $\gcd(k; n) = 1$.*
- **Corollary 1.4.5.** *The number of generators of a cyclic group of order n is $\phi(n)$.*

1.Introduction

- ◉ **Proposition 1.4.6.** *Let G be a finite group and let $a \in G$. Then the order of a is the number of elements in $\langle a \rangle$.*
- ◉ **Definition.** If G is a finite group, then the number of elements in G , denoted by $|G|$, is called the ***order of G*** .

2. Normal subgroups, quotient groups

- 2.1. Cosets
- 2.2. Theorem of Lagrange
- 2.3. Normal Subgroups
- 2.4. Quotient Groups

2. Normal subgroups, quotient groups

2.1. Cosets

- Let (G, \cdot) be a group with subgroup H . For $a, b \in G$, we say that a is ***congruent to b modulo H*** , and write $a \equiv b \pmod{H}$ if and only if $ab^{-1} \in H$.
- Proposition 2.1. 1.** *The relation $a \equiv b \pmod{H}$ is an equivalence relation on G . The equivalence class containing a can be written in the form $Ha = \{ha \mid h \in H\}$, and it is called a right coset of H in G . The element a is called a representative of*

2. Normal subgroups, quotient groups

- **Example 2.1.1. Find the right cosets of A_3 in S_3 .**

Solution. One coset is the subgroup itself $A_3 = \{(1), (123), (132)\}$. Take any element not in the subgroup, say (12) . Then another coset is $A_3(12) = \{(12), (123)(12), (132)(12)\} = \{(12), (13), (23)\}$. Since the right cosets form a partition of S_3 and the two cosets above contain all the elements of S_3 , it follows that these are the only two cosets

2. Normal subgroups, quotient groups

- **Example 2.1.2. Find the right cosets of $H = \{e, g^4, g^8\}$ in $C_{12} = \{e, g, g^2, \dots, g^{11}\}$.**
- *Solution.* H itself is one coset. Another is $Hg = \{g, g^5, g^9\}$. These two cosets have not exhausted all the elements of C_{12} , so pick an element, say g^2 , which is not in H or Hg . A third coset is $Hg^2 = \{g^2, g^6, g^{10}\}$ and a fourth is $Hg^3 = \{g^3, g^7, g^{11}\}$.

Since $C_{12} = H \cup Hg \cup Hg^2 \cup Hg^3$, these are all the cosets

2. Normal subgroups, quotient groups

- **2.2. Theorem of Lagrange**
- As the examples above suggest, every coset contains the same number of elements. We use this result to prove the famous theorem of Joseph Lagrange (1736–1813).
- **Lemma 2.2.1.** *There is a bijection between any two right cosets of H in G .*

Proof. Let Ha be a right coset of H in G . We produce a bijection between Ha and H , from which it follows that there is a bijection between any two right cosets.

Define $\psi: H \rightarrow Ha$ by $\psi(h) = ha$. Then ψ is clearly surjective. Now suppose that $\psi(h_1) = \psi(h_2)$, so that $h_1a = h_2a$. Multiplying each side by a^{-1} on the right, we obtain $h_1 = h_2$. Hence ψ is a bijection.

2. Normal subgroups, quotient groups

○ **Theorem 2.2.2.** *Lagrange's Theorem.* If G is a finite group and H is a subgroup of G , then $|H|$ divides $|G|$.

Proof. The right cosets of H in G form a partition of G , so G can be written as a disjoint union

$G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_k$ for a finite set of elements $a_1, a_2, \dots, a_k \in G$.

By Lemma 2.2.1, the number of elements in each coset is $|H|$. Hence, counting all the elements in the disjoint union above, we

2. Normal subgroups, quotient groups

- If H is a subgroup of G , the number of distinct right cosets of H in G is called the *index of H in G* and is written $|G : H|$. The following is a direct consequence of the proof of Lagrange's theorem.
- **Corollary 2.2.3.** *If G is a finite group with subgroup H , then*
$$|G : H| = |G| / |H|.$$
- **Corollary 2.2.4.** *If a is an element of a finite group G , then the order of a divides the order of G .*

2. Normal subgroups, quotient groups

2.3. Normal Subgroups

- Let G be a group with subgroup H . The *right cosets* of H in G are equivalence classes under the relation $a \equiv b \pmod{H}$, defined by $ab^{-1} \in H$. We can also define the relation L on G so that aLb if and only if $b^{-1}a \in H$. This relation, L , is an equivalence relation, and the equivalence class containing a is the *left coset* $aH = \{ah \mid h \in H\}$. As the following example shows the left coset of an

2. Normal subgroups, quotient groups

- **Example 2.3.1.** Find the left and right cosets of $H = A_3$ and $K = \{(1), (12)\}$ in S_3 .
- *Solution.* We calculated the right cosets of $H = A_3$ in Example 2.1.1.

Right Cosets

$$H = \{(1), (123), (132)\}; H(12) = \{(12), (13), (23)\}$$

Left Cosets

$$H = \{(1), (123), (132)\}; (12)H = \{(12), (23), (13)\}$$

In this case, the left and right cosets of H are the same.

- However, the left and right cosets of K are not all the same.

Right Cosets

$$K = \{(1), (12)\}; K(13) = \{(13), (132)\}; K(23) = \{(23), (123)\}$$

Left Cosets

$$K = \{(1), (12)\}; (23)K = \{(23), (132)\}; (13)K = \{(13), (123)\}$$

2. Normal subgroups, quotient groups

Definition: A subgroup H of a group G is called a *normal subgroup* of G if $g^{-1}hg \in H$ for all $g \in G$ and $h \in H$.

Proposition 2.3.1. $Hg = gH$, for all $g \in G$, if and only if H is a normal subgroup of G .

Proof. Suppose that $Hg = gH$. Then, for any element $h \in H$, $hg \in Hg = gH$. Hence $hg = gh_1$ for some $h_1 \in H$ and $g^{-1}hg = g^{-1}gh_1 = h_1 \in H$. Therefore, H is a normal subgroup.

Conversely, if H is normal, let $hg \in Hg$ and $g^{-1}hg = h_1 \in H$. Then $hg = gh_1 \in gH$ and $Hg \subseteq gH$. Also, $ghg^{-1} = (g^{-1})^{-1}hg^{-1} = h_2 \in H$, since H is normal, so $gh = h_2g \in Hg$. Hence, $gH \subseteq Hg$, and so $Hg = gH$.

2. Normal subgroups, quotient groups

- If N is a normal subgroup of a group G , the left cosets of N in G are the same as the right cosets of N in G , so there will be no ambiguity in just talking about the cosets of N in G .
- **Theorem 2.3.2.** *If N is a normal subgroup of (G, \cdot) , the set of cosets $G/N = \{Ng \mid g \in G\}$ forms a group $(G/N, \cdot)$, where the operation is defined by $(Ng_1) \cdot (Ng_2) = N(g_1 \cdot g_2)$. This group is called the quotient*

2. Normal subgroups, quotient groups

- Proof. The operation of multiplying two cosets, Ng_1 and Ng_2 , is defined in terms of particular elements, g_1 and g_2 , of the cosets. For this operation to make sense, we have to verify that, if we choose different elements, h_1 and h_2 , in the same cosets, the product coset $N(h_1 \cdot h_2)$ is the same as $N(g_1 \cdot g_2)$. In other words, we have to show that multiplication of cosets is well defined. Since h_1 is in the same coset as g_1 , we have $h_1 \equiv g_1 \pmod{N}$. Similarly, $h_2 \equiv g_2 \pmod{N}$. We show that $Nh_1h_2 = Ng_1g_2$. We have $h_1g_1^{-1} = n_1 \in N$ and $h_2g_2^{-1} = n_2 \in N$, so $h_1h_2(g_1g_2)^{-1} = h_1h_2g_2^{-1}g_1^{-1} = n_1g_1n_2g_2g_2^{-1}g_1^{-1} = n_1g_1n_2g_1^{-1}$. Now N is a normal subgroup, so $g_1n_2g_1^{-1} \in N$ and $n_1g_1n_2g_1^{-1} \in N$. Hence $h_1h_2 \equiv g_1g_2 \pmod{N}$ and $Nh_1h_2 = Ng_1g_2$. Therefore, the operation is well defined.*

2. Normal subgroups, quotient groups

- The operation is associative because $(Ng_1 \cdot Ng_2) \cdot Ng_3 = N(g_1g_2) \cdot Ng_3 = N(g_1g_2)g_3$ and also $Ng_1 \cdot (Ng_2 \cdot Ng_3) = Ng_1 \cdot N(g_2g_3) = Ng_1(g_2g_3) = N(g_1g_2)g_3$.
- Since $Ng \cdot Ne = Nge = Ng$ and $Ne \cdot Ng = Ng$, the identity is $Ne = N$.
- The inverse of Ng is Ng^{-1} because $Ng \cdot Ng^{-1} = N(g \cdot g^{-1}) = Ne = N$ and also $Ng^{-1} \cdot Ng = N$.
- Hence $(G/N, \cdot)$ is a group.

2. Normal subgroups, quotient groups

- **Example 2.3.1.** $(\mathbb{Z}_n, +)$ is the quotient group of $(\mathbb{Z}, +)$ by the subgroup $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$.
- *Solution.* Since $(\mathbb{Z}, +)$ is abelian, every subgroup is normal. The set $n\mathbb{Z}$ can be verified to be a subgroup, and the relationship $a \equiv b \pmod{n\mathbb{Z}}$ is equivalent to $a - b \in n\mathbb{Z}$ and to $n \mid a - b$. Hence $a \equiv b \pmod{n\mathbb{Z}}$ is the same relation as $a \equiv b \pmod{n}$. Therefore, \mathbb{Z}_n is the quotient group $\mathbb{Z}/n\mathbb{Z}$, where the operation on congruence classes is defined by $[a] + [b] = [a + b]$. $(\mathbb{Z}_n, +)$ is a cyclic group with 1 as a generator. When there is no confusion, we write the elements of \mathbb{Z}_n as $0, 1, 2, 3, \dots, n - 1$ instead of $[0], [1], [2], [3], \dots, [n - 1]$.

3. Homomorphisms.

- ③ 3.1. Definition of Homomorphisms
- ③ 3.2. Examples of Homomorphisms
- ③ 3.3. Theorem on Homomorphisms

3. Homomorphisms

- 3.1. Definition of Homomorphisms
- If (G, \cdot) and $(H, *)$ are two groups, the function $f : G \rightarrow H$ is called a *group homomorphism* if
$$f(a \cdot b) = f(a) * f(b) \text{ for all } a, b \in G.$$
- We often use the notation $f : (G, \cdot) \rightarrow (H, *)$ for such a homomorphism. Many authors use *morphism* instead of *homomorphism*.
- A *group isomorphism* is a bijective group homomorphism. If there is an isomorphism between the groups (G, \cdot) and $(H, *)$, we say that (G, \cdot) and $(H, *)$ are *isomorphic* and write $(G, \cdot) \cong (H, *)$.

3. Homomorphisms

- 3.2. Examples of Homomorphisms

- The function $f : \mathbb{Z} \rightarrow \mathbb{Z}_n$, defined by $f(x) = [x]$ is the group homomorphism.
- Let be P the group of all real numbers with operation addition, and let P^+ be the group of all positive real numbers with operation multiplication. The function $f : P \rightarrow P^+$, defined by $f(x) = e^x$, is a homomorphism, for if $x, y \in P$, then $f(x + y) = e^{x+y} = e^x e^y = f(x) f(y)$. Now f is an isomorphism, for its inverse function $g : P^+ \rightarrow P$ is $\ln x$. Therefore, the additive group P is isomorphic to the multiplicative group P^+ . Note that the inverse function g is also an isomorphism: $g(xy) = \ln(xy) = \ln x + \ln y = g(x) + g(y)$.

3. Homomorphisms

- 3.3. Theorem on Homomorphisms
- **Proposition 3.3.1.** *Let $f : G \rightarrow H$ be a group morphism, and let e_G and e_H be the identities of G and H , respectively. Then*
 - (i) $f(e_G) = e_H$.
 - (ii) $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$.
- *Proof.* (i) Since f is a morphism, $f(e_G)f(e_G) = f(e_G e_G) = f(e_G) = f(e_G)e_H$. Hence (i) follows by cancellation in H
- (ii) $f(a) f(a^{-1}) = f(a a^{-1}) = f(e_G) = e_H$ by (i). Hence $f(a^{-1})$ is the unique inverse of $f(a)$; that is $f(a^{-1}) = f(a)^{-1}$

3. Homomorphisms

- If $f : G \rightarrow H$ is a group morphism, the *kernel* of f , denoted by $\text{Ker}f$, is defined to be the set of elements of G that are mapped by f to the identity of H . That is, $\text{Ker}f = \{g \in G \mid f(g) = e_H\}$
- **Proposition 3.3.2.** *Let $f : G \rightarrow H$ be a group morphism. Then:*
 - (i) *$\text{Ker}f$ is a normal subgroup of G .*
 - (ii) *f is injective if and only if $\text{Ker}f = \{e_G\}$.*
- **Proposition 3.3.3.** *For any group morphism $f : G \rightarrow H$, the image of f , $\text{Im}f = \{f(g) \mid g \in G\}$, is a subgroup of H (although not necessarily normal).*

3. Homomorphisms

- **Theorem 3.3.4. Morphism Theorem for Groups.** *Let K be the kernel of the group morphism $f : G \rightarrow H$. Then G/K is isomorphic to the image of f , and the isomorphism*

$\psi : G/K \rightarrow \text{Im} f$ is defined by $\psi(Kg) = f(g)$.

- This result is also known as the **first isomorphism theorem**.

- *Proof.* The function ψ is defined on a coset by using one particular element in the coset, so we have to check that ψ is well defined; that is, it does not matter which element we use. If $Kg' = Kg$, then $g' \equiv g \pmod{K}$ so $g'g^{-1} = k \in K = \text{Ker} f$. Hence $g' = kg$ and so

$$f(g') = f(kg) = f(k)f(g) = e_H f(g) = f(g).$$

Thus ψ is well defined on cosets.

3. Homomorphisms

- The function ψ is a morphism because
$$\psi(Kg_1Kg_2) = \psi(Kg_1g_2) = f(g_1g_2) = f(g_1)f(g_2) = \psi(Kg_1)\psi(Kg_2).$$
- If $\psi(Kg) = e_H$, then $f(g) = e_H$ and $g \in K$. Hence the only element in the kernel of ψ is the identity coset K , and ψ is injective. Finally, $\text{Im}\psi = \text{Im}f$, by the definition of ψ . Therefore, ψ is the required isomorphism between G/K and $\text{Im}f$

3. Homomorphisms

- **Example 3.3.1.** Show that the quotient group P/Z is isomorphic to the circle group $W = \{e^{i\theta} \in X \mid \theta \in P\}$.

Solution. The set W consists of points on the circle of complex numbers of unit modulus, and forms a group under multiplication. Define the function

$f : \mathbb{R} \rightarrow W$ by $f(x) = e^{2\pi i x}$. This is a morphism from $(P, +)$ to

(W, \cdot) because

$$f(x + y) = e^{2\pi i(x+y)} = e^{2\pi i x} \cdot e^{2\pi i y} = f(x) \cdot f(y).$$

The morphism f is clearly surjective, and its kernel is $\{x \in P \mid e^{2\pi i x} = 1\} = Z$.

Therefore, the morphism theorem implies that $P/Z \cong W$.

Unit –III Combinatorics

- Basics of counting
- Permutations and Combinations
- Combinations with Repetitions
- Binomial coefficients
- Principles of inclusion and exclusion
- Pigeon hole principle and its application

- **Sum Rule:** If E_1, E_2, \dots, E_n are mutually exclusive events, and E_1 can happen in e_1 ways, E_2 can happen in e_2 ways, \dots , E_n can happen in e_n ways, then $(E_1 \text{ or } E_2 \text{ or } \dots \text{ or } E_n)$ can happen in $(e_1 + e_2 + \dots + e_n)$ ways.
- Ex. A man can spend his evening in one of the following ways.
He can do shopping or he can go to a Cinema hall or he can go to a restaurant.
If there are 6 shopping complexes, 8 cinema halls and 9 restaurants then, how many different ways he can spend his evening?.
- Solution: By Sum rule, he can spend his evening in $6 + 8 + 9 = 23$
different ways.

Ex.: If two distinguishable dice are rolled, then
a) How many ways can we get a sum of 4 or of 8
b) How many ways we get an even sum?

■ Solution: a) There are 3 ways to get a sum of 4

i.e., $\{(1, 3), (2, 2), (3, 1)\}$

Likewise, There are 5 ways to get a sum of 8.

i.e., $\{(2, 6), (3, 5), (4, 4), (5, 3), (6, 2)\}$.

The number of ways to get a sum of 4 or 8 = $3 + 5 = 8$

■ b) The number of ways we get an even sum =

The number of ways to get a sum of 2 or 4 or 6 or 8 or 10 or 12 =

$$1 + 3 + 5 + 5 + 3 + 1 = 18 \text{ ways .}$$

Ex. If two indistinguishable dice are rolled, then
a) How many ways can we get a sum of 4 or of 8 .
b) How many ways we get an even sum?.

- Solution: a) If the dice are identical, the outcomes (a,b) and (b,a) cannot be differentiated.

Now, there are only 2 ways to get a sum of 4

i.e., $\{(1, 3), (2, 2)\}$

Likewise, There are only 3 ways to get a sum of 8.

i.e., $\{(2, 6), (3, 5), (4, 4)\}$.

The number of ways to get a sum of 4 or 8 = $2 + 3 = 5$

- b) Likewise, The number of ways we get an even sum =

The number of ways to get a sum of 2 or 4 or 6 or 8 or 10 or 12 =

$$1 + 2 + 3 + 3 + 2 + 1 = 12 \text{ways} .$$

- **Product Rule:** If events E_1, E_2, \dots, E_n can happen in e_1, e_2, \dots, e_n ways respectively, then the sequence of events (E_1 first, followed by E_2, \dots , followed by E_n) can happen $(e_1 \cdot e_2 \cdot \dots \cdot e_n)$ ways.
- Ex. a) If 2 distinguishable dice are rolled, in how many ways can they fall?
b) If 5 distinguishable dice are rolled, how many possible outcomes are there?.
- Solution: a) The first die can fall in 6 ways and the second can fall in
6 ways.
 \therefore By product rule, the number of possible outcomes = $6 \cdot 6 = 36$.

- b) Similarly, the number of possible outcomes when 5 distinguishable dice are rolled = $6 \cdot 6 \cdot 6 \cdot 6 \cdot 6 = 6^5$
- Ex. A man wants to spend his evening in the following way.
First, He would like to do some shopping ,
then he would like to go to a Cinema hall and
finally he would like to go to a restaurant.
If there are 6 shopping complexes, 8 cinema halls and 9 restaurants then, how many different ways he can spend his evening?.
- Ans. $6 \cdot 8 \cdot 9 = 432$ ways.

Ex. a) How many 3-digit numbers can be formed using the digits
1,3,4,5,6,8 and 9?

b) How many 3-digit numbers can be formed if no digit can be
repeated?

- Solution: a) Here, each of the 3 digits can be filled in 7 ways .
∴ By product rule, The required number of 3-digit
numbers that can be formed = $7.7.7 = 343$.
- b) If the repetitions are not allowed,
The required number of 3-digit numbers that can be
formed =
$$7.6.5 = 210.$$

Ex. How many three digit even numbers are there which are even and have no repeated digits? (Here we are using all digits 0 through 9)

- Solution: An even number must end with 0,2,4,6,or 8.

- Case1

$$\begin{array}{r} x \quad x \quad 0 \\ 9 \quad 8 \quad - \end{array}$$

The number of 3- digit even numbers ending with 0 = $9 \cdot 8 = 72$

- Case2

$$\begin{array}{r} x \quad x \quad x \\ 8 \quad 8 \quad 4 \end{array}$$

The number of 3-digit even numbers not ending with 0 = $8 \cdot 8 \cdot 4 = 256$.

Since, these two cases are mutually exclusive, By sum rule

The required number of 3-digit even numbers = $72 + 256 = 328$.

- Ex. How many 4 digit even numbers have all 4 digits distinct ?
- Ans. 2296

Permutations

- **Permutations:** A permutation of n objects taken r at a time (also called an r -permutation of n objects) is an ordered selection or arrangement of r of the objects.
- $P(n, r) =$ The number of permutations of n objects taken r at a time
(without any repetitions).
- $P(n, 1) = n.$
- $P(n, 2) = n.(n - 1).$
- $P(n, 3) = n.(n - 1).(n - 2).$
-
- $P(n, r) = n.(n - 1)(n - 2).....\{n - (r - 1)\} = n! / (n - r)!$
- $P(n, n) = n!$ i.e., there are $n!$ Permutations of n objects.

Permutations

- **Note:**

- 1) There are $(n - 1)!$ permutations of n distinct objects around a circle.
- 2) $U(n, r) =$ The number of r -permutations of n objects with unlimited repetitions $= n^r$.
- 3) The number of permutations of n objects of which n_1 are alike, n_2 are alike, \dots , n_r are alike is
$$\frac{n!}{n_1! \cdot n_2! \cdot \dots \cdot n_r!}$$
- 4) The number of ways to arrange 'n' different pearls in a necklace is $(n - 1)! / 2$.

Ordered and unordered partitions

- 5) The number of ordered partitions of a set S of type $\{q_1, q_2, \dots, q_k\}$
where $|S| = n$ is
$$p(n; q_1, q_2, \dots, q_t) = \frac{n!}{q_1! q_2! \dots q_t!}$$
- 6) Enumeration of unordered partitions of equal cell size:
The number of unordered partitions of a set S of type (q, q, \dots, q) ,
(where $|S| = n = q \cdot t$) is
$$= \frac{n!}{(q!)^t \cdot t!}$$

Combinations

- **Combinations:**

- A combination of n-objects taken r at a time (called an r-combination of n objects) is an unordered selection of n objects.

- $C(n, r)$ = The number of combinations of n-objects taken r at time

- $C(n, r) = \frac{n!}{r! \cdot (n-r)!}$ (without repetitions)

- $n! = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 1$

- $r! = r \cdot (r-1) \cdot (r-2) \cdot \dots \cdot 1$

- **Note:** 1) $P(n, r) = r! \cdot C(n, r)$

- 2) $C(n, 0) = 1$

- 3) $C(n, 1) = n$

Combinations

- 4) $C(n, 2) = \frac{n \cdot (n - 1)}{1 \cdot 2}$
- 5) $C(n, 3) = \frac{n \cdot (n - 1) \cdot (n - 2)}{1 \cdot 2 \cdot 3}$
- 6) $C(n, n) = 1$
- 7) $C(n, r) = C(n, n - r)$

Combinations with repetitions

- $V(n, r)$ = The number of combinations of n distinct objects taken r at a time with unlimited repetitions.
- $V(n, r) = C(n - 1 + r, r)$
 $= C(n - 1 + r, n - 1)$
- $V(n, r)$ = The number of ways distributing ' r ' similar balls into ' n ' numbered boxes.
- $V(n, r)$ = The number of non negative integral solutions to the equation $x_1 + x_2 + \dots + x_n = r$
- $V(n, r)$ = The number of binary sequences with ' $n - 1$ ' ones and ' r ' zeros.

Examples

- Ex. How many ways are there to distributive 10 different books among 15 people, if no person is to receive more than one book?
a) $P(15, 10)$ b) $C(15, 10)$ c) 10^{15} d) 15^{10}
- Ans. a
- Ex. How many binary sequences are there of length 15?
a) 2^{15} b) $15!$ c) $P(15, 2)$ d) $C(15, 2)$
- Ans. a
- Ex. How many binary sequences are there of length 15 with exactly
6 ones and 9 zeros?
a) $P(15, 6)$ b) $C(15, 6)$ c) 2^6 d) $P(15, 6) \cdot C(15, 9)$
- Ans. b

Example

- Ex. A multiple choice test has 15 questions and 4 choices for each answer.
 - a) How many ways can the 15 questions be answered?
 - b) How many ways the 15 questions be answered so that exactly 3 answers are correct?
 - c) How many ways the 15 questions be answered so that at least 3 answers are correct?
- Solution:
- a) Since, each question can be answered in 4 ways, By product rule,
the 15 questions can be answered in 4^{15} ways.

- b) The 3 correct answers can be chosen in $C(15, 3)$ ways. Each of the remaining questions can be wrongly answered in 3 ways.

\therefore The required number of ways = $C(15, 3) \cdot 3^{12}$.

- c) The 15 questions can be answered in 4^{15} ways.

Number of ways in which at most 2 answers are correct =

$$3^{15} + C(15, 1) \cdot 3^{14} + C(15, 2) \cdot 3^{13}$$

The number of ways the 15 questions be answered so that at least 3

$$\text{answers are correct} = 4^{15} - \{3^{15} + C(15, 1) \cdot 3^{14} + C(15, 2) \cdot 3^{13}\}$$

Ex. How many ways can 10 similar balls be placed in six numbered boxes?

- Solution: The number of ways distributing 'r' similar balls into 'n'

$$\text{numbered boxes} = V(n, r) = C(n - 1 + r, r).$$

Here, $n = 6$ and $r = 10$

$$\begin{aligned}\therefore \text{The required number of ways} &= V(6, 10) \\ &= C(15, 10) \\ &= C(15, 5) \\ &= 3003.\end{aligned}$$

Ex. How many non negative integral solutions are there to the equation

$$x_1 + x_2 + x_3 + x_4 + x_5 = 50 .$$

- Solution: The number of non negative integral solutions to the equation $\{x_1 + x_2 + x_3 + \dots + x_n = r\} =$
$$V(n, r) = C(n-1 + r, r).$$

Here, $n = 5$ and $r = 50$

$$\begin{aligned} \therefore \text{The required number of solutions} &= V(5, 50) \\ &= C(54, 50) \\ &= C(54, 4) = 3,16,251. \end{aligned}$$

Ex. How many binary sequences are possible with ten one's and five zeros.

- Solution: The number of binary sequences with 'n - 1' ones and 'r' zeros = $V(n, r)$

Here, $n - 1 = 10$ and $r = 5$.

$$\begin{aligned}\therefore \text{Required number of binary sequences} &= V(11, 5) \\ &= C(15, 5) = 3003.\end{aligned}$$

Ex. In how many ways can 5 similar books be placed on 3 different shelves so that each shelf contains at least one book ?

- Solution: First, let us place one book in each of the shelves to ensure that each shelf contains at least one of the books.
- Now, let us count the number of ways of distributing the remaining two books in 3 shelves.
- \therefore Required number of ways = $V(3, 2)$
 $= C(4, 2) = 10.$

Ex. A professor wishes to conduct a test with 10 questions. In how many ways can the test be given a total of 30 marks if each question is to be worth 2 or more marks?

- Solution: Since each question has to carry at least 2 marks, First he has to allot 2 marks for each question.
- Now let us count the number of ways of distributing the remaining 10 marks to 10 questions.
- \therefore Required number of ways = $V(10, 10)$
 $= C(19, 10).$

Ex. How many non negative integral solutions are there to

$$x_1 + x_2 + x_3 + x_4 + x_5 = 20$$

where $x_1 \geq 3$, $x_2 \geq 2$, $x_3 \geq 4$, $x_4 \geq 6$ and $x_5 \geq 0$?

- Solution: This problem is similar to, placing 20 similar balls in 5 numbered boxes so that, first box contains at least 3 balls, second box contains at least 2 balls, third box contains at least 4 balls and fourth box contains at least 6 balls.
- First, let us place 3 balls in the first box, 2 balls in the second, 4 balls in the third and 6 balls in the fourth box.
- Now, let us count the number of ways of distributing the remaining 5 balls in boxes.
- \therefore Required number of solutions = $V(5, 5)$
 $= C(9, 5) = C(9, 4) = 126.$

Ex. How many non negative integral solutions are there to the inequality
 $x_1 + x_2 + x_3 + x_4 + x_5 \leq 19$?.

- Solution: If k is some integer between 0 and 19, then for every distribution of k balls into 5 boxes, one could distribute the remaining $19 - k$ balls into a sixth box.
- Hence, the number of non negative integral solutions of $x_1 + x_2 + x_3 + x_4 + x_5 \leq 19$ is the same as the number of negative integral solutions of $x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 19$.
- \therefore Required number of solutions = $V(6, 19)$
 $= C(24, 19) = C(24, 5)$.

Ex. Find the number of ways in which 16 apples can be distributed among four persons so that each of them gets at least one apple ?

Ans. 455 (Home work)

Ex. How many 5 letter words can be formed from the word 'DADDY' ?

a) 20

b) 120

c) 15

d) 80

■ Solution: Required number of words = $\frac{5!}{3!} = 20.$

■ Ans. a

Ex. How many 10-permutations are there of {a,a,a, b,b,b,b, c,c, d} ?

a) 12, 600

b) 16, 200

c) 14, 620

d) 8, 400

■ Solution:

■ Required number of permutations = $\frac{10!}{3! \cdot 4! \cdot 2!} = 12,600.$

■ Ans. a

Ordered and unordered partitions

- Ex. In how many ways can 14 men be partitioned into 6 teams where the first team has 3 members, the second team has 2 members, the third team has 3 members, the fourth, fifth and sixth teams each have 2 members.

- Solution: The required number of ordered partitions =

- $$P(14: 3,2,3,2,2,2)$$

- $$= \frac{14!}{3! \cdot 2! \cdot 3! \cdot 2! \cdot 2! \cdot 2!}$$

- $$= \frac{14!}{3! \cdot 2! \cdot 3! \cdot 2! \cdot 2! \cdot 2!}$$

Ex. In how many ways can 12 of the 14 men be partitioned into 3 teams where the first team has 3 members, the second team has 5 members and the third team has 4 members.

■ Solution:

■ The number of ways 12 men can be chosen out of 14 = $C(14, 12)$.

■ The number of ordered partitions = $P(12; 3, 5, 4) = \frac{12!}{3! \cdot 5! \cdot 4!}$

■ \therefore Required number of ways = $C(14, 2) \cdot \frac{12!}{3! \cdot 5! \cdot 4!}$

Ex. In how many ways can 12 of the 14 men be partitioned into 3 teams of 4 each?

■ Solution:

■ The number of ways 12 men can be chosen out of 14 = $C(14, 12)$.

■ The number of unordered partitions = $P(12; 4,4,4) = \frac{12!}{(4!)^3 \cdot 3!}$

■ \therefore Required number of ways = $C(14, 12) \cdot \frac{12!}{(4!)^3 \cdot 3!}$

■

Ex. In how many ways can 14 men be partitioned into 6 teams where two teams have 3 each and four teams have 2 each?

■ Solution:

■ Required number of unordered partitions = $\frac{14!}{(3!)^2 \cdot 2! \cdot (2!)^4 \cdot 4!}$

■

- Ex. Suppose that there are 101 players entered in a single elimination tennis tournament. How many matches must be conducted to declare the winner ?
- a) 101 b) 100 c) 99 d) 51
- Solution: Since each match eliminates one player,
- we have a one-to one correspondence between the the number of losers and the number of matches to be conducted.
- \therefore The required number of matches to be conducted to declare the winner = 100.
- Ans. b

Binomial Coefficients

- **Notation:**

- $C(n, 0) = C_0 = 1,$

- $C(n, 1) = C_1 = n,$

- $C(n, 2) = C_2 = \{n.(n - 1)\} / \{1.2\},$

-,

- $C(n, r) = C_r = \{n.(n - 1).(n - 2) \dots (n - r + 1)\} / \{1.2.3 \dots r\},$

-

- $C(n, n) = C_n = 1$

- $C(n, r) =$ The number of combinations of n-objects taken r at time

- (without repetitions).

- $$= \frac{n!}{r! \cdot (n-r)!}$$

- 1. Give a combinatorial proof for the following.

a) $C(n, r) \cdot C(r, k) = C(n, k) \cdot C(n - k, r - k)$ for integers $n \geq r \geq k \geq 0$.

(Newton's identity).

b) $C(n, r) \cdot r = n \cdot C(n - 1, r - 1)$.

- Proof: a) The L.H.S. counts the number of ways of selecting two sets: first a set of r objects and then from A , a set of k objects.
- For example, we may be counting the number of ways to select a committee of r people and then to select a subset of k leaders from this committee.
- On the other hand, the R.H.S. counts the the number of ways we select a group of k leaders from the n people first, and then select remaining $r - k$ people from the remaining $n - k$ people.

-
- $\therefore \text{L.H.S.} = \text{R.H.S.}$
 - b) putting $k = 1$ in the Newton's Identity, we have
$$\text{C}(n, r) \cdot \text{C}(r, 1) = \text{C}(n, 1) \cdot \text{C}(n - 1, r - 1).$$
 - $\Rightarrow \text{C}(n, r) \cdot r = n \cdot \text{C}(n - 1, r - 1).$

The Binomial Theorem

- Let n be a positive integer. Then for all x and y
- $(x + y)^n = C(n, 0) \cdot x^n + C(n, 1) \cdot x^{n-1} \cdot y + C(n, 2) \cdot x^{n-2} \cdot y^2 + \dots$
- $+ C(n, r) \cdot x^{n-r} \cdot y^r + \dots + C(n, n) \cdot y^n .$

- $$= \sum_{r=0}^n C(n, r) x^{n-r} \cdot y^r .$$

- $$(x + 1)^n = \sum_{r=0}^n C(n, r) x^r .$$

- $$(1 - x)^n = \sum_{r=0}^n C(n, r) (-1)^r \cdot x^r .$$

- 8) $C_0 - C_1 + C_2 - C_3 + \dots + (-1)^n C_n = 0$



- 9) $(C_0 + C_2 + C_4 + \dots) = (C_1 + C_3 + C_5 + \dots) = 2^{n-1}$

- 10) $C_1 + 2C_2 + 3C_3 + \dots + n C_n = n 2^{n-1}$

- 10) $C_1 - 2 C_2 + 3 C_3 - \dots + (-1)^{n-1} n.C_n = 0$

n

- 11) Prove that $\sum_{r=0}^n C(n, r) 2^r = 3^n$

- We know that,

n

- $(x + 1)^n = \sum_{r=0}^n C(n, r) x^r$. Putting $x = 2$, we have

n

- $3^n = \sum_{r=0}^n C(n, r) 2^r$

a) 2^n

b) 2^{2n}

Ex. $C(2n, 0) + C(2n, 1) + \dots + C(2n, 2n) =$

c) 2^{n+2}

d) $n 2^n$

■ Ans. B

■ Vandermonde's Identity :

■ Prove that $C(n+m, r) = C(n, 0).C(m, r) + C(n, 1) . C(m, r - 1) + \dots$

■ $\dots + C(n,r). C(m,0).$ (for integers $m \geq n \geq 0$)

■ Proof: (Give combinatorial proof)

■ Hint: Let S be the union set of m men and n women.

Ex. Prove that $\{C(n, 0) + C(n, 1) + \dots + C(n, r) + \dots + C(n, n)\}^2 = C(2n, 0) + C(2n, 1) + \dots + C(2n, 2n)$

■ Consider $(1+x)^{2n} = C(2n, 0) + C(2n, 1).x + \dots + C(2n, 2n)x^{2n}$
 ... (1)

■ Again, $(1+x)^{2n} = [(1+x)^n]^2 = \{C(n, 0) + C(n, 1).x + \dots + C(n, r).x^r + \dots + C(n, n).x^n\}^2$... (2)

From (1) and (2), we have

$$\{C(n, 0) + C(n, 1).x + \dots + C(n, n).x^n\}^2 = C(2n, 0) + C(2n, 1).x + \dots + C(2n, 2n)x^{2n} \dots (3)$$

Putting $x = 1$ in (3), we have

■ $\{C(n, 0) + C(n, 1) + \dots + C(n, r) + \dots + C(n, n)\}^2 = C(2n, 0) + C(2n, 1) + \dots + C(2n, 2n)$

■ Hence, the result follows.

The Multinomial Theorem

- State and prove the multinomial theorem.
- Statement: Let n be a positive integer. Then for all x_1, x_2, \dots, x_t , we have

$$(x_1 + x_2 + \dots + x_t)^n = \sum P(n; q_1, q_2, \dots, q_t) \cdot (x_1^{q_1} x_2^{q_2} \dots x_t^{q_t})$$

Where the summation extends over all sets of non negative integers q_1, q_2, \dots, q_t where $q_1 + q_2 + \dots + q_t = n$.

There are $C(n + t - 1, n)$ terms in the expansion of $(x_1 + x_2 + \dots + x_t)^n$

- Proof: The coefficient of $(x_1^{q_1} x_2^{q_2} \dots x_t^{q_t})$ is the number of ways of arranging the n letters $\{q_1 \cdot x_1, q_2 \cdot x_2, \dots, q_t \cdot x_t\}$, therefore it is $P(n; q_1, q_2, \dots, q_t)$.

-
- The number of terms is determined as follows: each term of the form $x_1^{q_1} x_2^{q_2} \dots x_t^{q_t}$ is a selection of n objects with repetitions from t distinct types.
 - Hence there are $C(n + t - 1, n)$ ways to do this.

- Ex. In the expansion of $(x_1 + x_2 + x_3 + x_4 + x_5)^{10}$
- a) Evaluate the coefficient of $x_1^2 x_3 x_4^3 x_5^4$
- b) How many terms are there in the expansion ?

■ Solution: a) The coefficient of $x_1^2 x_3 x_4^3 x_5^4$ is

■
$$P(10 ; 2, 0, 1, 3, 4) = \frac{10!}{2! 0! 1! 3! 4!} = 12,600$$

- b) The number of terms in the expansion = $C(10 + 5 - 1, 10)$
- $$= C(14, 4) = 1001$$

Ex. In the expansion of $(2x - 3y + 5z)^8$

a) Evaluate the coefficient of $x^3 y^3 z^2$

b) How many terms are there in the expansion ?

-
- Solution:a) Let $x_1 = 2x$, $x_2 = -3y$, $x_3 = 5z$ then
 - The coefficient of $x_1^3 x_2^3 x_3^2 = P(8 ; 3, 3, 2) = \frac{8!}{3! 3! 2!} = 560$
 - Thus, the coefficient of $x^3 y^3 z^2 = 2^3 (-3)^3 \cdot 5^2 \cdot P(8 ; 3, 3, 2)$
 $= - (5400) \cdot (560)$
 - b) The number of terms in the expansion $= C(8 + 3 - 1, 8)$
 $= C(10, 2) = 45$

Ex. Use the multinomial theorem to expand $(x - 2y + z)^3$

- $(x - 2y + z)^3 = P(3; 3,0,0) x^3 + P(3; 0,3,0) (-2y)^3 + P(3; 0,0,3) z^3 +$
- $P(3; 2,1,0) x^2 (-2y) + P(3; 1,2,0) x (-2y)^2 +$
- $P(3; 2,0,1) x^2 z + P(3; 1,0,2) x z^2 +$
- $P(3; 0,2,1) (-2y)^2 z + P(3; 0,1,2) (-2y) z^2 +$
- $P(3; 1,1,1) x(-2y) z .$

- $= x^3 - 8y^3 + z^3 - 6x^2y + 12xy^2 + 3x^2z + 3xz^2 + 12y^2z - 6yz^2 - 12xyz$

Ex. What is the coefficient of $x^3 y^7$ in

a) $(x + y)^{10}$

b) $(2x - 9y)^{10}$

-
- Solution: a) The coefficient of $x^3 y^7 = \frac{10!}{3! 7!} = 120$
 -
 - b) The coefficient of $x^3 y^7 = 2^3 \cdot (-9)^7 \cdot \frac{10!}{3! 7!}$
 -

The Principle of Inclusion-Exclusion:

- Theorem: If A and B are subsets of some universe set U , then

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

- $$= |A \cap B^c| + |B \cap A^c| + |A \cap B| .$$

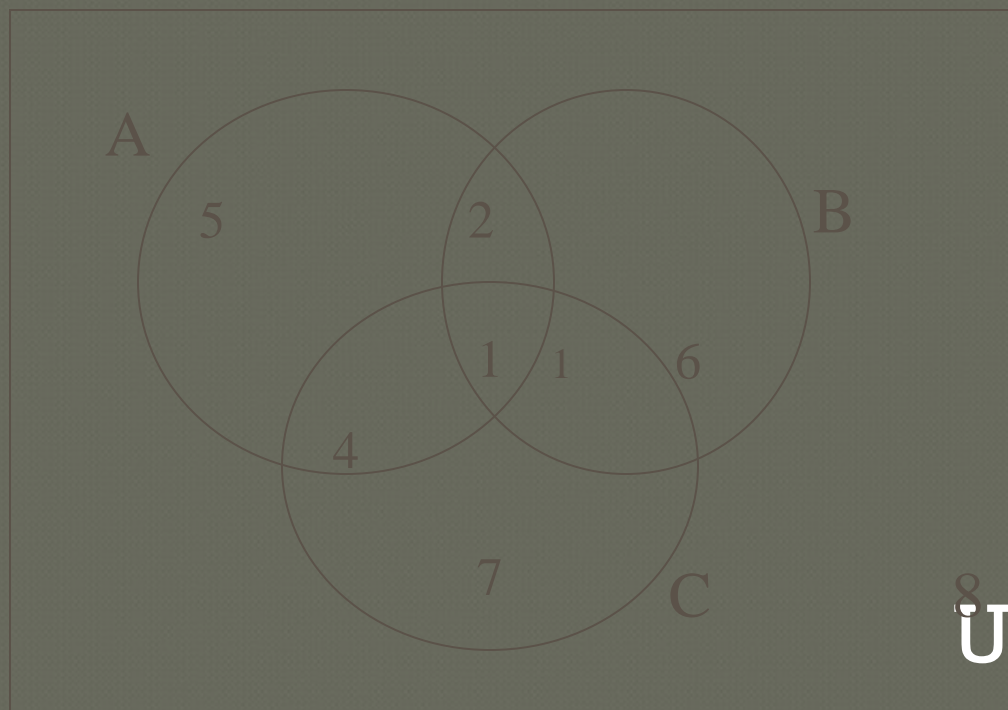
- Theorem: If A , B and C are finite sets, then

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



1) $A \cap B \cap C$ 2) $\bar{A} \cap \bar{B} \cap C$ 3) $A \cap B \cap \bar{C}$ 4) $A \cap \bar{B} \cap C$

5) $A \cap \bar{B} \cap \bar{C}$ 6) $\bar{A} \cap B \cap \bar{C}$ 7) $\bar{A} \cap \bar{B} \cap C$ 8) $\bar{A} \cap B \cap C$



Ex. Suppose that 200 faculty members can speak French and 50 can speak Russian, while only 20 can speak both French and Russian. How many faculty members can speak either French or Russian ?

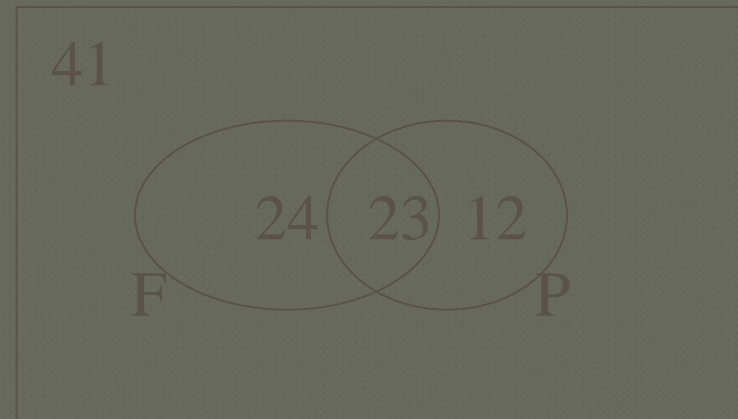
- Solution: Let F = Set of faculty who can speak French.
- R = Set of faculty who can speak Russian.
- $F \cap R$ = Set of faculty who can speak French and Russian.
- \therefore Required number of faculty members = $|F \cup R|$
- $|F \cup R| = |F| + |R| - |F \cap R|$.
- $= 200 + 50 - 20$
- $= 230$.

Example

- Ex. If there are 200 faculty members that speak French, 50 that speak Russian, 100 that speak Spanish, 20 that speak French and Russian, 60 that speak French and Spanish, 35 that speak Russian and Spanish, while only 10 speak French, Russian and Spanish. How many speak either French or Russian or Spanish ?
- Solution: Let F = Set of faculty who can speak French.
- R = Set of faculty who can speak Russian.
- S = Set of faculty who can speak Spanish.
- \therefore Required number of faculty members = $|F \cup R \cup S|$
 $= |F| + |R| + |S| - |F \cap R| - |R \cap S| - |S \cap F| + |F \cap R \cap S|.$
 $= 200 + 50 + 100 - 20 - 60 - 35 + 10 = 245.$

Ex. A certain computer center employs 100 computer programmers. Of these 47 can program in FORTRAN , 35 in Pascal and 23 can program in both languages. How many can program in neither of these 2 languages?

■ **Solution:**



- The number of programmers who can program in at least one of the 2 languages = $24 + 23 + 12 = 59$.
- The number of programmers who can program in neither of these 2 languages = $100 - 59 = 41$.

- Let $F = \{\text{Programmers who can program in FORTRAN}\}$
- $P = \{\text{Programmers who can program in Pascal}\}$
- $F \cap P = \{\text{Programmers who can program in FORTRAN and Pascal}\}$
- The number of programmers who can program in at least one of the 2 languages = $|F \cup P|$
- $= |F| + |P| - |F \cap P|$
- $= 47 + 35 - 23 = 59.$
- \therefore The number of programmers who can program in neither of these 2 languages = $F^c \cap P^c = (F \cup P)^c = |U| - |F \cup P|$
- $= 100 - 59 = 41.$

Ex. In the previous example,

- a) How many can program in only one of the 2 languages?
 - b) How many can program in Pascal but not in FORTRAN.
 - c) How many can program in FORTRAN but not in Pascal.
-

- Solution: From the Venn diagram, we have
- a) The number of programmers who can program in only one of the 2 languages = $24 + 12 = 36$.
- b) The number of programmers who can program in Pascal but not in FORTRAN = 12.
- c) The number of programmers who can program in FORTRAN but not in Pascal = 24.

Euler's ϕ -function

- **Euler's ϕ - function:**
- If n is a positive integer, then
- $\phi(n)$ = The number of integers 'x' such that $1 \leq x \leq n$ and such that
n and x are relatively prime.
- $\phi(n) = n \left[\left\{1 - \left(\frac{1}{p_1}\right)\right\} \cdot \left\{1 - \left(\frac{1}{p_2}\right)\right\} \cdot \dots \cdot \left\{1 - \left(\frac{1}{p_k}\right)\right\} \right]$
where p_1, p_2, \dots, p_k are distinct prime divisors of n .
- Ex. Find the number of positive integers less than or equals to 91 and
relatively prime to 91.
- Solution: The prime divisors of 91 are 7 and 13.
- $\phi(91) = 91 \cdot \left\{1 - \left(\frac{1}{7}\right)\right\} \cdot \left\{1 - \left(\frac{1}{13}\right)\right\}$.
- $= 72$.

Ex. Find the number of positive integers less than or equals to 100 and relatively prime to 100.

- Solution: The prime divisors of 2 and 5.
- $\phi(100) = 100 \cdot \{1 - (1/2)\} \cdot \{1 - (1/5)\}.$
- $= 40.$
-

Derangements

- **Derangements:**
- Among the permutations of $\{1, 2, \dots, n\}$ there are some, called derangements, in which none of the n integers appears in its natural place.
- $D_n =$ The number of derangements of n elements

-
-
-

$$= n! \left(\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} + \dots + \frac{(-1)^n}{n!} \right)$$

Ex. Five balls marked with B_1, B_2, B_3, B_4, B_5 are to be kept in 5 cells marked with C_1, C_2, C_3, C_4, C_5 . How many ways this can be done so that ball B_i is not kept in cell C_i ($i = 1, 2, \dots, 5$).

■ Solution: Required number of ways = D_5

■ =

■ $5! \left[\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} \right]$

■ = $60 - 20 + 5 - 1 = 44.$

Ex. Four students take a quiz. Then for the purpose of grading, the teacher ask the students to exchange papers, so that no one is grading his own paper. How many ways this can be done?.

■ Solution: Required number of ways = D_4

■ =

■ $4! \left[\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} \right]$

■ = $12 - 4 + 1 = 9.$

- Ex. Let 5 different books be distributed to 5 students. Suppose the books are returned and distributed to the students again later on . In how many ways the books be distributed so that no student will get the same book twice ?
- Solution: The number of ways 5 different books be distributed to 5 students $= 5! = 120$.
- Second time, the number of ways the books be distributed so that no student will get the same book twice $= D_5 = 44$.
- \therefore The required number of distributions $= (120) \cdot (44)$
- $= 5280$.

The pigeonhole principle

- Suppose a flock of pigeons fly into a set of pigeonholes to roost
- If there are more pigeons than pigeonholes, then there must be at least 1 pigeonhole that has more than one pigeon in it
- If $k+1$ or more objects are placed into k boxes, then there is at least one box containing two or more of the objects
 - This is Theorem 1

Pigeonhole principle examples

- In a group of 367 people, there must be two people with the same birthday
 - As there are 366 possible birthdays
- In a group of 27 English words, at least two words must start with the same letter
 - As there are only 26 letters

Generalized pigeonhole principle

- If N objects are placed into k boxes, then there is at least one box containing $\lceil N/k \rceil$ objects
 - This is Theorem 2

Generalized pigeonhole principle examples

- ◉ Among 100 people, there are at least $\lceil 100/12 \rceil = 9$ born on the same month
- ◉ How many students in a class must there be to ensure that 6 students get the same grade (one of A, B, C, D, or F)?
 - The “boxes” are the grades. Thus, $k = 5$
 - Thus, we set $\lceil N/5 \rceil = 6$
 - Lowest possible value for N is 26

examples

- A bowl contains 10 red and 10 yellow balls
- a) How many balls must be selected to ensure 3 balls of the same color?
 - One solution: consider the “worst” case
 - Consider 2 balls of each color
 - You can’t take another ball without hitting 3
 - Thus, the answer is 5
 - Via generalized pigeonhole principle
 - How many balls are required if there are 2 colors, and one color must have 3 balls?
 - How many pigeons are required if there are 2 pigeon holes, and one must have 3 pigeons?
 - number of boxes: $k = 2$
 - We want $\lceil N/k \rceil = 3$
 - What is the minimum N ?
 - $N = 5$

examples

- A bowl contains 10 red and 10 yellow balls
- b) How many balls must be selected to ensure 3 yellow balls?
 - Consider the “worst” case
 - Consider 10 red balls and 2 yellow balls
 - You can't take another ball without hitting 3 yellow balls
 - Thus, the answer is 13

examples

- 6 computers on a network are connected to at least 1 other computer
- Show there are at least two computers that have the same number of connections
- The number of boxes, k , is the number of computer connections
 - This can be 1, 2, 3, 4, or 5
- The number of pigeons, N , is the number of computers
 - That's 6
- By the generalized pigeonhole principle, at least one box must have $\lceil N/k \rceil$ objects
 - $\lceil 6/5 \rceil = 2$
 - In other words, at least two computers must have the same number of connections

examples

- Consider 5 distinct points (x_i, y_i) with integer values, where $i = 1, 2, 3, 4, 5$
- Show that the midpoint of at least one pair of these five points also has integer coordinates
- Thus, we are looking for the midpoint of a segment from (a,b) to (c,d)
 - The midpoint is $((a+c)/2, (b+d)/2)$
- Note that the midpoint will be integers if a and c have the same parity: are either both even or both odd
 - Same for b and d
- There are four parity possibilities
 - (even, even), (even, odd), (odd, even), (odd, odd)
- Since we have 5 points, by the pigeonhole principle, there must be two points that have the same parity possibility
 - Thus, the midpoint of those two points will have integer coordinates

Recurrence Relations

Recurrence Relations

A **recurrence relation** for the sequence $\{a_n\}$ is an equation that expresses a_n in terms of one or more of the previous terms of the sequence, namely, a_0, a_1, \dots, a_{n-1} , for all integers n with $n \geq n_0$, where n_0 is a nonnegative integer.

A sequence is called a **solution** of a recurrence relation if its terms satisfy the recurrence relation.

Recurrence Relations

In other words, a recurrence relation is like a recursively defined sequence, but **without specifying any initial values (initial conditions)**.

Therefore, the same recurrence relation can have (and usually has) **multiple solutions**.

If **both** the initial conditions and the recurrence relation are specified, then the sequence is **uniquely** determined.

Recurrence Relations

Example:

Consider the recurrence relation

$$a_n = 2a_{n-1} - a_{n-2} \text{ for } n = 2, 3, 4, \dots$$

Is the sequence $\{a_n\}$ with $a_n = 3n$ a solution of this recurrence relation?

For $n \geq 2$ we see that

$$2a_{n-1} - a_{n-2} = 2(3(n-1)) - 3(n-2) = 3n = a_n.$$

Therefore, $\{a_n\}$ with $a_n = 3n$ is a solution of the recurrence relation.

Recurrence Relations

Is the sequence $\{a_n\}$ with $a_n=5$ a solution of the same recurrence relation?

For $n \geq 2$ we see that

$$2a_{n-1} - a_{n-2} = 2 \cdot 5 - 5 = 5 = a_n.$$

Therefore, $\{a_n\}$ with $a_n=5$ is also a solution of the recurrence relation.

Modeling with Recurrence Relations

Example:

Someone deposits \$10,000 in a savings account at a bank yielding 5% per year with interest compounded annually. How much money will be in the account after 30 years?

Solution:

Let P_n denote the amount in the account after n years.

How can we determine P_n on the basis of P_{n-1} ?

Modeling with Recurrence Relations

We can derive the following **recurrence relation**:

$$P_n = P_{n-1} + 0.05P_{n-1} = 1.05P_{n-1}.$$

The initial condition is $P_0 = 10,000$.

Then we have:

$$P_1 = 1.05P_0$$

$$P_2 = 1.05P_1 = (1.05)^2P_0$$

$$P_3 = 1.05P_2 = (1.05)^3P_0$$

...

$$P_n = 1.05P_{n-1} = (1.05)^nP_0$$

We now have a **formula** to calculate P_n for any natural number n and can avoid the iteration.

Modeling with Recurrence Relations

Let us use this formula to find P_{30} under the initial condition $P_0 = 10,000$:

$$P_{30} = (1.05)^{30} \cdot 10,000 = 43,219.42$$

After 30 years, the account contains \$43,219.42.

Modeling with Recurrence Relations

Another example:

Let a_n denote the number of bit strings of length n that do not have two consecutive 0s (“valid strings”). Find a recurrence relation and give initial conditions for the sequence $\{a_n\}$.

Solution:

Idea: The number of valid strings equals the number of valid strings ending with a 0 plus the number of valid strings ending with a 1.

Modeling with Recurrence Relations

Let us assume that $n \geq 3$, so that the string contains at least 3 bits.

Let us further assume that we know the number a_{n-1} of valid strings of length $(n - 1)$. Then how many valid strings of length n are there, if the string ends with a 1?

There are a_{n-1} such strings, namely the set of valid strings of length $(n - 1)$ with a 1 appended to them.

Note: Whenever we append a 1 to a valid string, that string remains valid.

Modeling with Recurrence Relations

Now we need to know: How many valid strings of length n are there, if the string ends with a **0**?

Valid strings of length n ending with a **0 must have a 1 as their $(n - 1)$ st bit** (otherwise they would end with 00 and would not be valid).

And what is the number of valid strings of length $(n - 1)$ that end with a 1?

We already know that there are a_{n-1} strings of length n that end with a 1.

Therefore, there are a_{n-2} strings of length $(n -$

Modeling with Recurrence Relations

So there are a_{n-2} valid strings of length n that end with a 0 (all valid strings of length $(n - 2)$ with 10 appended to them).

As we said before, the number of valid strings is the number of valid strings ending with a 0 plus the number of valid strings ending with a 1.

That gives us the following **recurrence relation**:

$$a_n = a_{n-1} + a_{n-2}$$

Modeling with Recurrence Relations

What are the **initial conditions**?

$$a_1 = 2 \text{ (0 and 1)}$$

$$a_2 = 3 \text{ (01, 10, and 11)}$$

$$a_3 = a_2 + a_1 = 3 + 2 = 5$$

$$a_4 = a_3 + a_2 = 5 + 3 = 8$$

$$a_5 = a_4 + a_3 = 8 + 5 = 13$$

...

This sequence satisfies the same recurrence relation as the **Fibonacci sequence**.

Since $a_1 = f_3$ and $a_2 = f_4$, we have $a_n = f_{n+2}$.

Solving Recurrence Relations

In general, we would prefer to have an **explicit formula** to compute the value of a_n rather than conducting n iterations.

For one class of recurrence relations, we can obtain such formulas in a systematic way.

Those are the recurrence relations that express the terms of a sequence as **linear combinations** of previous terms.

Solving Recurrence Relations

Definition: A linear homogeneous recurrence relation of degree k with constant coefficients is a recurrence relation of the form:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k},$$

Where c_1, c_2, \dots, c_k are real numbers, and $c_k \neq 0$.

A sequence satisfying such a recurrence relation is uniquely determined by the recurrence relation and the k initial conditions

$$a_0 = C_0, a_1 = C_1, a_2 = C_2, \dots, a_{k-1} = C_{k-1}.$$

Solving Recurrence Relations

Examples:

The recurrence relation $P_n = (1.05)P_{n-1}$ is a linear homogeneous recurrence relation of **degree one**.

The recurrence relation $f_n = f_{n-1} + f_{n-2}$ is a linear homogeneous recurrence relation of **degree two**.

The recurrence relation $a_n = a_{n-5}$ is a linear homogeneous recurrence relation of **degree five**.

Solving Recurrence Relations

Basically, when solving such recurrence relations, we try to find solutions of the form $a_n = r^n$, where r is a constant.

$a_n = r^n$ is a solution of the recurrence relation

$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k}$ if and only if $r^n = c_1 r^{n-1} + c_2 r^{n-2} + \dots + c_k r^{n-k}$.

Divide this equation by r^{n-k} and subtract the right-hand side from the left:

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \dots - c_{k-1} r - c_k = 0$$

This is called the **characteristic equation** of the recurrence relation.

Solving Recurrence Relations

The solutions of this equation are called the **characteristic roots** of the recurrence relation.

Let us consider linear homogeneous recurrence relations of **degree two**.

Theorem: Let c_1 and c_2 be real numbers. Suppose that $r^2 - c_1r - c_2 = 0$ has two distinct roots r_1 and r_2 .

Then the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2}$ if and only if $a_n = \alpha_1r_1^n + \alpha_2r_2^n$ for $n = 0, 1, 2, \dots$, where α_1 and α_2 are constants.

Solving Recurrence Relations

Example: What is the solution of the recurrence relation $a_n = a_{n-1} + 2a_{n-2}$ with $a_0 = 2$ and $a_1 = 7$?

Solution: The characteristic equation of the recurrence relation is $r^2 - r - 2 = 0$.

Its roots are $r = 2$ and $r = -1$.

Hence, the sequence $\{a_n\}$ is a solution to the recurrence relation if and only if:

$a_n = \alpha_1 2^n + \alpha_2 (-1)^n$ for some constants α_1 and α_2 .

Solving Recurrence Relations

Given the equation $a_n = \alpha_1 2^n + \alpha_2 (-1)^n$ and the initial conditions $a_0 = 2$ and $a_1 = 7$, it follows that

$$a_0 = 2 = \alpha_1 + \alpha_2$$

$$a_1 = 7 = \alpha_1 \cdot 2 + \alpha_2 \cdot (-1)$$

Solving these two equations gives us

$$\alpha_1 = 3 \text{ and } \alpha_2 = -1.$$

Therefore, the solution to the recurrence relation and initial conditions is the sequence $\{a_n\}$ with

$$a_n = 3 \cdot 2^n - (-1)^n.$$

Solving Recurrence Relations

$a_n = r^n$ is a solution of the linear homogeneous recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k}$$

if and only if

$$r^n = c_1 r^{n-1} + c_2 r^{n-2} + \dots + c_k r^{n-k}.$$

Divide this equation by r^{n-k} and subtract the right-hand side from the left:

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \dots - c_{k-1} r - c_k = 0$$

This is called the **characteristic equation** of the recurrence relation.

Solving Recurrence Relations

The solutions of this equation are called the **characteristic roots** of the recurrence relation.

Let us consider linear homogeneous recurrence relations of **degree two**.

Theorem: Let c_1 and c_2 be real numbers. Suppose that $r^2 - c_1r - c_2 = 0$ has two distinct roots r_1 and r_2 .

Then the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2}$ if and only if $a_n = \alpha_1r_1^n + \alpha_2r_2^n$ for $n = 0, 1, 2, \dots$, where α_1 and α_2 are constants.

Solving Recurrence Relations

Example: Give an explicit formula for the Fibonacci numbers.

Solution: The Fibonacci numbers satisfy the recurrence relation $f_n = f_{n-1} + f_{n-2}$ with initial conditions $f_0 = 0$ and $f_1 = 1$.

The characteristic equation is $r^2 - r - 1 = 0$.

Its roots are

$$r_1 = \frac{1 + \sqrt{5}}{2}, \quad r_2 = \frac{1 - \sqrt{5}}{2}$$

Solving Recurrence Relations

Therefore, the Fibonacci numbers are given by

$$f_n = \alpha_1 \left(\frac{1 + \sqrt{5}}{2} \right)^n + \alpha_2 \left(\frac{1 - \sqrt{5}}{2} \right)^n$$

for some constants α_1 and α_2 .

We can determine values for these constants so that the sequence meets the conditions $f_0 = 0$ and $f_1 = 1$:

$$f_0 = \alpha_1 + \alpha_2 = 0$$

$$f_1 = \alpha_1 \left(\frac{1 + \sqrt{5}}{2} \right) + \alpha_2 \left(\frac{1 - \sqrt{5}}{2} \right) = 1$$

Solving Recurrence Relations

The unique solution to this system of two equations and two variables is

$$\alpha_1 = \frac{1}{\sqrt{5}}, \quad \alpha_2 = -\frac{1}{\sqrt{5}}$$

So finally we obtained an explicit formula for the Fibonacci numbers:

$$f_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n$$

Solving Recurrence Relations

But what happens if the characteristic equation has only one root?

How can we then match our equation with the initial conditions a_0 and a_1 ?

Theorem: Let c_1 and c_2 be real numbers with $c_2 \neq 0$. Suppose that $r^2 - c_1r - c_2 = 0$ has only one root r_0 .

A sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2}$ if and only if $a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n$, for $n = 0, 1, 2, \dots$, where α_1 and α_2 are constants.

Solving Recurrence Relations

Example: What is the solution of the recurrence relation $a_n = 6a_{n-1} - 9a_{n-2}$ with $a_0 = 1$ and $a_1 = 6$?

Solution: The only root of $r^2 - 6r + 9 = 0$ is $r_0 = 3$.

Hence, the solution to the recurrence relation is

$a_n = \alpha_1 3^n + \alpha_2 n 3^n$ for some constants α_1 and α_2 .

To match the initial condition, we need

$$a_0 = 1 = \alpha_1$$

$$a_1 = 6 = \alpha_1 \cdot 3 + \alpha_2 \cdot 3$$

Solving these equations yields $\alpha_1 = 1$ and $\alpha_2 = 1$.

Consequently, the overall solution is given by

$$a_n = 3^n + n 3^n.$$

Recurrence Relations

Generating Functions of Sequences

Sequences

$$A = \{a_r\}, r = 0 \dots \infty.$$

Examples:

1. $A = \{a_r\}, r = 0 \dots \infty$, where $a_r = 2^r$.
 $= \{1, 2, 4, 8, 16, \dots, 2^r, \dots\}$

2. $B = \{b_r\}, r = 0 \dots \infty$, where

$$\begin{aligned} b_r &= 0, \text{ if } 0 \leq r \leq 4 \\ &= 2, \text{ if } 5 \leq r \leq 9 \\ &= 3, \text{ if } r = 10 \\ &= 4, \text{ if } 11 \leq r \end{aligned}$$
$$= \{0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 3, 4, 4, \dots\}$$

3. $C = \{c_r\}, r = 0 .. \infty$, where $c_r = r + 1$.
 $= \{1, 2, 3, 4, 5, \dots\}$

4. $D = \{d_r\}, r = 0 .. \infty$, where $d_r = r^2$.
 $= \{0, 1, 4, 9, 16, 25, \dots\}$

Generating function for the sequence $\bar{A} = \{a_r\}, r = 0 \dots \infty$.

$$\begin{aligned} A(X) &= a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n + \dots \\ &= \sum a_r X^r, r = 0 \dots \infty. \end{aligned}$$

Examples:

1. Generating function for the sequence $\bar{A} = \{a_r\}, r = 0 \dots \infty$,

where $a_r = 2^r$.

$$\begin{aligned} A(X) &= 1 + 2X + 4X^2 + \dots + 2^n X^n + \dots \\ &= \sum 2^r X^r, r = 0 \dots \infty. \end{aligned}$$

2. Generating function for the sequence $B = \{b_r\}, r = 0 .. \infty$,
where

$$\begin{aligned} b_r &= 0, \text{ if } 0 \leq r \leq 4 \\ &= 2, \text{ if } 5 \leq r \leq 9 \\ &= 3, \text{ if } r = 10 \\ &= 4, \text{ if } 11 \leq r \end{aligned}$$

$$\begin{aligned} B(X) &= 2X^5 + 2X^6 + 2X^7 + 2X^8 + 2X^9 + 3X^{10} + 4X^{11} + \\ &4X^{12} + \dots + 4X^n + \dots \end{aligned}$$

3. Generating function for the sequence $C = \{c_r\}, r = 0 .. \infty$,
where $c_r = r + 1$.

$$\begin{aligned} C(X) &= 1 + 2X + 3X^2 + \dots + (n+1)X^n + \dots \\ &= \sum (r+1)X^r, r = 0 .. \infty. \end{aligned}$$

4. Generating function for the sequence $D = \{d_r\}, r = 0 .. \infty$,
where $d_r = r^2$.

$$\begin{aligned} D(X) &= X + 4X^2 + 9X^3 + 16X^4 + 25X^5 + \dots + n^2 X^n + \dots \\ &= \sum r^2 X^r, r = 0 .. \infty. \end{aligned}$$

Definitions

Let the Generating Functions / Formal Power Series be

$$A(X) = \sum a_r X^r, r = 0 \dots \infty.$$

$$\text{and } B(X) = \sum b_s X^s, s = 0 \dots \infty.$$

1. Equality

$$A(X) = B(X), \text{ iff } a_n = b_n \text{ for each } n \geq 0.$$

2. Multiplication by a scalar number C

$$C A(X) = \sum (C a_r) X^r, r = 0 \dots \infty.$$

3. Sum

$$A(X) + B(X) = \sum (a_n + b_n) X^n, n = 0 \dots \infty.$$

4. Product

$$A(X) B(X) = \sum P_n X^n, n = 0 \dots \infty,$$

$$\text{where } P_n = \sum_{j+k=n} a_j b_k.$$

Exercises:

1. Find a Generating function for the sequence

$A = \{a_r\}, r = 0 .. \infty$, where

$$a_r = 1, \text{ if } 0 \leq r \leq 2$$

$$= 3, \text{ if } 3 \leq r \leq 5$$

$$= 0, \text{ if } r \geq 6$$

$$A(X) = 1 + X + X^2 + 3X^3 + 3X^4 + 3X^5$$

2. Build a generating function for $a_r =$ no. of integral solutions to the equation $e_1 + e_2 + e_3 = r$, if $0 \leq e_i \leq 3$ for each i .

$$A(X) = (1 + X + X^2 + X^3)^3$$

3. Write a generating function for $a_r =$ no. of ways of selecting r balls from 3 red balls, 5 blue balls, and 7 white balls.

$$A(X) = (1 + X + X^2 + X^3) (1 + X + X^2 + X^3 + X^4 + X^5) (1 + X + X^2 + X^3 + X^4 + X^5 + X^6 + X^7)$$

4. Find the coefficient of X^{23} in $(1 + X^5 + X^9)^{10}$.

$$e_1 + e_2 + \dots + e_{10} = 23 \text{ where } e_i = 0, 5, 9.$$

$$1 \times 5 + 2 \times 9 + 7 \times 0 = 23$$

$$\begin{aligned} \text{Coefficient of } X^{23} &= 10! / (1! 2! 7!) \\ &= 10 \cdot 9 \cdot 8 / (2) \\ &= 10 \cdot 9 \cdot 4 \\ &= 360 \end{aligned}$$

5. Find the coefficient of X^{32} in $(1 + X^5 + X^9)^{10}$.

$$e_1 + e_2 + \dots + e_{10} = 32 \text{ where } e_i = 0, 5, 9.$$

$$1 \times 5 + 3 \times 9 + 6 \times 0 = 32$$

$$\begin{aligned} \text{Coefficient of } X^{32} &= 10! / (1! 3! 6!) \\ &= 10 \cdot 9 \cdot 8 \cdot 7 / (3 \cdot 2) \\ &= 10 \cdot 3 \cdot 4 \cdot 7 \\ &= 840 \end{aligned}$$

6. Find a Generating function for the no. of r -combinations of $\{3.a, 5.b, 2.c\}$.

$$A(X) = (1 + X + X^2 + X^3) (1 + X + X^2 + X^3 + X^4 + X^5) (1 + X + X^2)$$

Calculating Coefficient of generating function

If $A(X) = \sum a_r X^r, r = 0 \dots \infty$, then $A(X)$ is said to have a multiplicative inverse if there is $B(X) = \sum b_k X^k, k = 0 \dots \infty$ such that $A(X) B(X) = 1$.

$$a_0 b_0 = 1$$

$$a_1 b_0 + a_0 b_1 = 0$$

$$a_0 b_2 + a_1 b_1 + a_2 b_0 = 0$$

$$a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 = 0$$

...

$$a_0 b_2 + a_0 b_2 + \dots + a_0 b_2 = 0$$

...

$$b_0 = 1 / a_0$$

$$b_1 = -a_1 b_0 / a_0$$

$$b_2 = -a_1 b_1 - a_2 b_0 / a_0$$

...

Geometric Series

$$A(X) = 1 - X$$

$$a_0 = 1, a_1 = -1.$$

$$b_0 = 1 / a_0 = 1$$

$$b_1 = -a_1 b_0 / a_0 = -(-1) (1) / (1) = 1$$

$$b_2 = -a_1 b_1 - a_2 b_0 / a_0 = -(-1) (1) - (0) (1) / (1) = 1$$

...

$$\therefore b_i = 1$$

$$1 / (1 - X) = \sum X^r, r = 0 .. \infty.$$

Replace X by aX , where a is a real no.

$$1 / (1 - aX) = \sum a_r X^r, r = 0 .. \infty.$$

Let $a = -1$

$$1 / (1 + X) = \sum (-1)^r X^r, r = 0 .. \infty.$$

$$1 / (1 + aX) = \sum (-1)^r a_r X^r, r = 0 .. \infty.$$

$$\begin{aligned} 1 / (1 - X)^n &= (\sum X^k)^n, k = 0 .. \infty. \\ &= \sum C(n - 1 + r, r) X^r, r = 0 .. \infty. \end{aligned}$$

$$1 / (1 + X)^n = (\sum (-1)^r X^k)^n, k = 0 .. \infty.$$

$$= \sum C(n-1+r, r) (-1)^r X^r, r = 0 .. \infty.$$

$$1 / (1 - aX)^n = (\sum a^r X^k)^n, k = 0 .. \infty.$$

$$= \sum C(n-1+r, r) a^r X^r, r = 0 .. \infty.$$

$$1 / (1 - X^k) = \sum X^{kr}, k = 0 .. \infty.$$

$$1 / (1 + X^k) = \sum (-1)^r X^{kr}, k = 0 .. \infty.$$

$$1 / (a - X) = (1 / a) \sum X^r / a^r, r = 0 .. \infty.$$

$$1 / (X - a) = (-1 / a) \sum X^r / a^r, r = 0 .. \infty.$$

$$1 / (X + a) = (1 / a) \sum X^r / ((-1)^r a^r), r = 0 .. \infty.$$

$$1 + X + X^2 + \dots + X^n = (1 - X^{n+1}) / (1 - x)$$

Special Cases of Binomial Theorem

$$(1 + X)^n = 1 + C(n, 1) X + C(n, 2) X^2 + \dots + C(n, n) X^n$$

$$(1 + X^k)^n = 1 + C(n, 1) X^k + C(n, 2) X^{2k} + \dots + C(n, n) X^{nk}$$

$$(1 - X)^n = 1 - C(n, 1) X + C(n, 2) X^2 + \dots + (-1)^n C(n, n) X^n$$

$$(1 - X^k)^n = 1 - C(n, 1) X^k + C(n, 2) X^{2k} + \dots + (-1)^n C(n, n) X^{nk}$$

Examples:

1. Calculate $A(X) = \sum a_r X^r, r = 0 \dots \infty = 1 / (X^2 - 5X + 6)$.

$$(X^2 - 5X + 6) = (X - 3)(X - 2)$$

$$1 / (X^2 - 5X + 6) = A / (X - 3) + B / (X - 2)$$

$$\therefore A(X - 2) + B(X - 3) = 1$$

Let $X = 2$, Then $B = -1$

Let $X = 3$, Then $A = 1$

$$1 / (X^2 - 5X + 6)$$

$$= 1 / (X - 3) - 1 / (X - 2)$$

$$= (-1 / 3) \sum X^r / 3^r - (-1 / 2) \sum X^r / 2^r, r = 0 \dots \infty.$$

$$= (-1 / 3) \sum X^r / 3^r + (1 / 2) \sum X^r / 2^r, r = 0 \dots \infty.$$

2. Compute the coefficients of $A(X) = \sum a^r X^r, r = 0 \dots \infty$
 $= (X^2 - 5X + 3) / (X^4 - 5X^2 + 4).$

$$\begin{aligned}(X^4 - 5X^2 + 4) &= (X^2 - 1)(X^2 - 4) \\ &= (X - 1)(X + 1)(X - 2)(X + 2)\end{aligned}$$

$$\begin{aligned}(X^2 - 5X + 3) / (X^4 - 5X^2 + 4) \\ &= A / (X - 1) + B / (X + 1) + C / (X - 2) + D / (X + 2)\end{aligned}$$

$$\begin{aligned}\therefore (X^2 - 5X + 3) &= A(X + 1)(X - 2)(X + 2) \\ &\quad + B(X - 1)(X - 2)(X + 2) \\ &\quad + C(X - 1)(X + 1)(X + 2) \\ &\quad + D(X - 1)(X + 1)(X - 2)\end{aligned}$$

For $X = 1, A = 1 / 6$

For $X = -1, B = 3 / 2$

For $X = 2, C = -1 / 4$

For $X = -2, D = -17 / 12$

$$\therefore (X^2 - 5X + 3) / (X^4 - 5X^2 + 4)$$

$$= 1/(6(X - 1)) + 3/(2(X + 1)) - 1/(4(X - 2)) - 17/(12(X + 2))$$

$$= (-1/6)\sum X^r + 3/2\sum (-1)^r X^r - 1/4(-1/2)\sum X^r / 2^r$$

$$17/12(1/2)\sum X^r / ((-1)^r 2^r), r = 0 .. \infty$$

$$= \sum [(-1/6) + 3/2(-1)^r + 1/8(1/2^r) - 17/24(-1)^r / 2^r] X^r, r = 0 .. \infty$$

3. Find the coefficient of X^{20} in $(X^3 + X^4 + X^5 + \dots)^5$.

$$(X^3 + X^4 + X^5 + \dots)^5$$

$$= [X^3 (1 + X + X^2 + \dots)]^5$$

$$= X^{15} (\sum X^r)^5, r = 0 \dots \infty$$

$$= X^{15} \sum C(5 - 1 + r, r) X^r, r = 0 \dots \infty$$

$$= X^{15} \sum C(4 + r, r) X^r, r = 0 \dots \infty$$

Coefficient of X^{20} in $(X^3 + X^4 + X^5 + \dots)^5$

$$= \text{Coefficient of } X^5 \text{ in } \sum C(4 + r, r) X^r, r = 0 \dots \infty$$

$$\therefore r = 5$$

$$C(4 + r, r)$$

$$= C(9, 5)$$

$$= 9! / (5! 4!)$$

$$= 9 \cdot 8 \cdot 7 \cdot 6 / (4 \cdot 3 \cdot 2)$$

$$= 9 \cdot 7 \cdot 2$$

$$= 126$$

Recurrence relations

Recurrence relation

Formula that relates for any integer $n \geq 1$, the n th term of a sequence

$A = \{a_r\}$, $r = 0 \dots \infty$ to one or more of the terms a_0, a_1, \dots, a_{n-1} .

Examples

$$a_n + 5a_{n-1} + 6a_{n-2} = 0.$$

$$a_n + 5a_{n-1} + 6a_{n-2} = 3n^2 - 2n + 1.$$

Linear recurrence relation

A recurrence relation of the form

$c_0(n) + c_1(n)a_n + \dots + c_k(n) a_{n-k} = f(n)$ for $n \geq k$,
where $c_0(n), c_1(n), \dots, c_k(n)$, and $f(n)$ are functions of n .

Example

$$a_n - (n-1)a_{n-1} - (n-1)a_{n-2} = 5n.$$

Linear recurrence relation of degree k

$c_0(n)$ and $c_k(n)$ are not identically zero.

Example

$$a_n + 5a_{n-1} + 6a_{n-2} = 0.$$

Linear recurrence relation with constant coefficients

$c_0(n), c_1(n), \dots, c_k(n)$ are constants.

Example

$$a_n + 5a_{n-1} + 6a_{n-2} = 0.$$

Homogeneous recurrence relation

$f(n)$ is identically zero.

Example

$$a_n + 5a_{n-1} + 6a_{n-2} = 0.$$

Inhomogeneous recurrence relation

$f(n)$ is not identically zero.

Example

$$a_n + 5a_{n-1} + 6a_{n-2} = 5n.$$

Solving recurrence relation by substitution and Generating functions

Solving recurrence relation by substitution / Backtracking

Technique for finding an explicit formula for the sequence defined by a recurrence relation.

Backtrack the value of a_n by substituting the definition of a_{n-1} , a_{n-2} , ... until a pattern is clear.

Examples

1. Use the technique of *backtracking*, to find an explicit formula for the sequence defined by the recurrence relation and initial condition for

$$a_n = a_{n-1} + 3, a_1 = 2.$$

$$a_n = a_{n-1} + 3$$

$$= (a_{n-2} + 3) + 3$$

$$= ((a_{n-3} + 3) + 3) + 3 = a_{n-3} + 3.3$$

...

$$\text{or } a_n = a_{n-1} + 1.3$$

$$= a_{n-2} + 2.3$$

...

$$= a_{n-(n-1)} + (n-1).3$$

$$= a_1 + (n-1).3$$

$$= 2 + (n-1).3$$

∴ The explicit formula for the sequence is

$$a_n = 2 + (n-1).3$$

2. Use the technique of *backtracking*, to find an explicit formula for the sequence defined by the recurrence relation and initial condition for $a_n = 2.5a_{n-1}$, $a_1 = 4$.

$$\begin{aligned}a_n &= 2.5a_{n-1} \\ &= 2.5(2.5a_{n-2}) \\ &= (2.5)^2a_{n-2} \\ &= (2.5)^3a_{n-3} \\ &\quad \dots \\ &= (2.5)^{n-1}a_{n-(n-1)} \\ &= (2.5)^{n-1}a_1 \\ &= 4(2.5)^{n-1}\end{aligned}$$

\therefore Explicit formula is $a_n = 4(2.5)^{n-1}$

3. Use the technique of *backtracking*, to find an explicit formula for the sequence defined by the recurrence relation and initial condition for $a_n = 5a_{n-1} + 3$, $a_1 = 3$.
-

$$\begin{aligned} a_n &= 5a_{n-1} + 3 \\ &= 5(5a_{n-2} + 3) + 3 \\ &= 5^2 a_{n-2} + (5 + 1)3 \\ &= 5^2 (5a_{n-3} + 3) + (5 + 1)3 \\ &= 5^3 a_{n-3} + (5^2 + 5 + 1)3 \\ &\quad \dots \\ &= 5^{n-1} a_{n-(n-1)} + (5^{n-2} + \dots + 5^2 + 5 + 1)3 \\ &= 5^{n-1} a_1 + (5^{n-2} + \dots + 5^2 + 5 + 1)3 \\ &= 5^{n-1} 3 + (5^{n-2} + \dots + 5^2 + 5 + 1)3 \\ &= (5^{n-1} + 5^{n-2} + \dots + 5^2 + 5 + 1)3 \\ &= 3(5^n - 1) / 4 \end{aligned}$$

\therefore Explicit formula is $a_n = 3(5^n - 1) / 4$

4. Use the technique of *backtracking*, to find an explicit formula for the sequence defined by the recurrence relation and initial condition for $a_n = a_{n-1} + n$, $a_1 = 4$.

$$\begin{aligned} a_n &= a_{n-1} + n \\ &= a_{n-2} + (n-1) + n \\ &= a_{n-3} + (n-2) + (n-1) + n \\ &\quad \dots \\ &= a_{n-(n-1)} + [n - (n-1) + 1] + \dots + (n-1) + n \\ &= a_1 + 2 + \dots + (n-1) + n \\ &= a_1 - 1 + [1 + 2 + \dots + (n-1) + n] \\ &= 4 - 1 + n(n+1)/2 \\ &= 3 + n(n+1)/2 \end{aligned}$$

\therefore Explicit formula is $a_n = 3 + n(n+1)/2$

Solving recurrence relations by Generating functions

Shifting properties of generating functions

$$\begin{aligned} X^k A(X) &= X^k \sum a_n X^n, n = 0 .. \infty \\ &= \sum a_n X^{n+k}, n = 0 .. \infty \end{aligned}$$

Replacing $n+k$ by r , we get

$$\sum a_{r-k} X^r, r = k .. \infty$$

Equivalent expressions for generating functions

If $A(X) = \sum a_n X^n, n = 0 .. \infty$, then

$$\sum a_n X^n, n = k .. \infty = A(X) - a_0 - a_1 X - \dots - a_{k-1} X^{k-1}.$$

$$\sum a_{n-1} X^n, n = k .. \infty = X(A(X) - a_0 - a_1 X - \dots - a_{k-2} X^{k-2}).$$

$$\sum a_{n-2} X^n, n = k .. \infty = X^2(A(X) - a_0 - a_1 X - \dots - a_{k-3} X^{k-3}).$$

$$\sum a_{n-3} X^n, n = k .. \infty = X^3(A(X) - a_0 - a_1 X - \dots - a_{k-4} X^{k-4}).$$

...

$$\sum a_{n-k} X^n, n = k .. \infty = X^k(A(X)).$$

Examples

- 1. Solve the *recurrence relation* $a_n - 7 a_{n-1} + 10 a_{n-2} = 0, n \geq 0,$
 $a_0 = 10, a_1 = 41,$ using *generating functions*.
-

1. Let $A(X) = \sum a_n X^n, n = 0 .. \infty.$

2. Multiply each term in the recurrence relation by X^n and sum from
2 to $\infty.$

$$\sum a_n X^n - 7 \sum a_{n-1} X^n + 10 \sum a_{n-2} X^n = 0, n = 2 .. \infty.$$

3. Replace each infinite sum by an equivalent expression.

$$[A(X) - a_0 - a_1 X] - 7X[A(X) - a_0] + 10X^2[A(X)] = 0.$$

4. Simplify.

$$A(X)(1 - 7X + 10X^2) = a_0 + a_1 X - 7 a_0 X.$$

$$\begin{aligned} A(X) &= [a_0 + (a_1 - 7 a_0)X] / (1 - 7X + 10X^2) \\ &= [a_0 + (a_1 - 7 a_0)X] / [(1 - 2X)(1 - 5X)] \end{aligned}$$

5. Decompose $A(X)$ as a sum of partial fractions.

$$A(X) = C_1 / (1 - 2X) + C_2 / (1 - 5X)$$

6. Express $A(X)$ as a sum of familiar series.

$$\begin{aligned} A(X) &= C_1 \sum 2^n X^n + C_2 \sum 5^n X^n, n = 0 \dots \infty. \\ &= \sum (C_1 2^n + C_2 5^n) X^n, n = 0 \dots \infty. \end{aligned}$$

7. Express a_n as the coefficient of X^n in $A(X)$ and in the sum of the other series.

$$a_n = C_1 2^n + C_2 5^n.$$

8. Determine the values of C_1 and C_2 .

$$\text{For } n = 0, a_0 = C_1 + C_2 = 10 \quad \dots (1)$$

$$\text{For } n = 1, a_1 = 2 C_1 + 5 C_2 = 41 \quad \dots (2)$$

Solving (1) and (2), we get

$$C_1 = 3$$

$$C_2 = 7$$

$$\therefore a_n = (3) 2^n + (7) 5^n.$$

- 2. Solve the *recurrence relation* $a_n - 9 a_{n-1} + 26 a_{n-2} - 24 a_{n-3} = 0$, $n \geq 3$, $a_0 = 0$, $a_1 = 1$, and $a_2 = 10$ using *generating functions*.
-

1. Let $A(X) = \sum a_n X^n$, $n = 0 \dots \infty$.

2. Multiply each term in the recurrence relation by X^n and sum from 3 to ∞ .

$$\sum_{n=3}^{\infty} a_n X^n - 9 \sum_{n=3}^{\infty} a_{n-1} X^n + 26 \sum_{n=3}^{\infty} a_{n-2} X^n - 24 \sum_{n=3}^{\infty} a_{n-3} X^n = 0,$$

3. Replace each infinite sum by an equivalent expression.

$$[A(X) - a_0 - a_1 X - a_2 X^2] - 9X [A(X) - a_0 - a_1 X] - 26X^2 [A(X) - a_0] - 24X^3 [A(X)] = 0.$$

4. Simplify.

$$\begin{aligned} & A(X)(1 - 9X + 26X^2 - 24X^3) \\ &= a_0 + a_1 X + a_2 X^2 - 9 a_0 X - 9 a_1 X^2 + 26 a_0 X^2. \\ A(X) &= [a_0 + (a_1 - 9 a_0) X + (a_2 - 9 a_1 + 26 a_0) X^2] / \\ & \quad (1 - 9X + 26X^2 - 24X^3) \\ &= [a_0 + (a_1 - 9 a_0) X + (a_2 - 9 a_1 + 26 a_0) X^2] / \\ & \quad [(1 - 2X)(1 - 3X)(1 - 4X)] \end{aligned}$$

5. Decompose $A(X)$ as a sum of partial fractions.

$$A(X) = C_1 / (1 - 2X) + C_2 / (1 - 3X) + C_3 / (1 - 4X)$$

6. Express $A(X)$ as a sum of familiar series.

$$\begin{aligned} A(X) &= C_1 \sum 2^n X^n + C_2 \sum 3^n X^n + C_3 \sum 4^n X^n, n = 0 \dots \infty. \\ &= \sum (C_1 2^n + C_2 3^n + C_2 3^n + C_3 4^n) X^n, n = 0 \dots \infty. \end{aligned}$$

7. Express a_n as the coefficient of X^n in $A(X)$ and in the sum of the other series.

$$a_n = C_1 2^n + C_2 3^n + C_3 4^n.$$

8. Determine the values of C_1 , C_2 and C_3 .

Substituting $a_0 = 0$, $a_1 = 1$, and $a_2 = 10$ in step 4, we get

$$\begin{aligned} A(X) &= [X + X^2] / [(1 - 2X)(1 - 3X)(1 - 4X)] \\ &= C_1 / (1 - 2X) + C_2 / (1 - 3X) + C_3 / (1 - 4X) \\ \text{i.e., } C_1(1 - 3X)(1 - 4X) &+ C_2(1 - 2X)(1 - 4X) \\ &+ C_3(1 - 2X)(1 - 3X) = X + X^2 \end{aligned}$$

$$\text{for } X = 1/2, C_1 = 3/2$$

$$\text{for } X = 1/3, C_2 = -4$$

$$\text{for } X = 1/4, C_3 = 5/2$$

$$\therefore a_n = (3/2) 2^n - (4) 3^n + (5/2) 4^n .$$

Exercises

1. Solve the *recurrence relation* $a_n - a_{n-1} - 9 a_{n-2} + 9 a_{n-3} = 0, n \geq 3,$
 $a_0 = 0, a_1 = 1,$ and $a_2 = 2$ using *generating functions*.
2. Solve the *recurrence relation* $a_n - 3 a_{n-2} + 2 a_{n-3} = 0, n \geq 3, a_0 = 1,$
 $a_1 = 0,$ and $a_2 = 0$ using *generating functions*

Method of Characteristics roots

Characteristic equation for a linear homogeneous recurrence

relation of degree k , $a_n = r_1 a_{n-1} + \dots + r_k a_{n-k}$ is

$$x^k = r_1 x^{k-1} + r_2 x^{k-2} + \dots + r_k.$$

1. Characteristic equation $x^2 - r_1 x - r_2 = 0$ of the recurrence relation

$a_n = r_1 a_{n-1} + r_2 a_{n-2}$, having two distinct roots s_1 and s_2 .

Explicit formula for the sequence is $a_n = us_1^n + vs_2^n$ and u and v depend on the initial conditions.

2. Characteristic equation $x^2 - r_1 x - r_2 = 0$ of the recurrence relation

$a_n = r_1 a_{n-1} + r_2 a_{n-2}$ having a single root s .

Explicit formula for the sequence is $a_n = us^n + vns^n$ and u and v depend on the initial conditions.

Examples

1. Solve the *recurrence relation* $a_n = 4a_{n-1} + 5a_{n-2}$, $a_1 = 2$, $a_2 = 6$.

The associated equation is $x^2 - 4x - 5 = 0$

$$\text{i.e. } (x - 5)(x + 1) = 0$$

\therefore The different roots are $s_1 = 5$ and $s_2 = -1$.

Explicit formula is $a_n = us_1^n + vs_2^n$

$$a_1 = u(5) + v(-1) = 5u - v$$

Given $a_1 = 2$

$$\therefore 5u - v = 2 \quad (1)$$

$$a_2 = u(5)^2 + v(-1)^2 = 25u + v$$

Given $a_2 = 6$

$$\therefore 25u + v = 6 \quad (2)$$

Solving the equations (1) and (2), we get

$$u = 4/15 \text{ and } v = -2/3$$

$$\begin{aligned} \therefore \text{Explicit formula is } a_n &= us_1^n + vs_2^n \\ &= 4/15(5)^n - 2/3(-1)^n \end{aligned}$$

2. Solve the *recurrence relation* $a_n = -6a_{n-1} - 9a_{n-2}$,
 $a_1 = 2.5, a_2 = 4.7$.

The associated equation is $x^2 + 6x + 9 = 0$
i.e. $(x + 3)^2 = 0$

\therefore The multiple root is $s = -3$.

Explicit formula is $a_n = us^n + vs^n$
 $a_1 = u(-3) + v(-3) = -3u + 3v$

Given $a_1 = 2.5$
 $\therefore -3u + 3v = 2.5$ (1)

$a_2 = u(-3)^2 + v(-3)^2 = 9u + 18v$

Given $a_2 = 4.7$
 $\therefore 9u + 18v = 4.7$ (2)

Solving the equations (1) and (2), we get
 $u = -19.7/9$ and $v = 12.2/9$

\therefore Explicit formula is $a_n = us^n + vns^n$
 $= (-19.7/9)(-3)^n + (12.2/9)n(-3)^n$

3. Solve the recurrence relation $a_n = 2a_{n-2}$, $a_1 = \sqrt{2}$, $a_2 = 6$.

The associated equation is $x^2 - 2 = 0$

$$\text{i.e. } (x - \sqrt{2})(x + \sqrt{2}) = 0$$

\therefore The different roots are $s_1 = \sqrt{2}$ and $s_2 = -\sqrt{2}$.

Explicit formula is $a_n = us_1^n + vs_2^n$

$$a_1 = u(\sqrt{2}) + v(-\sqrt{2}) = \sqrt{2}u - \sqrt{2}v$$

Given $a_1 = \sqrt{2}$

$$\therefore \sqrt{2}u - \sqrt{2}v = \sqrt{2}$$

$$u - v = 1 \quad (1)$$

$$a_2 = u(\sqrt{2})^2 + v(-\sqrt{2})^2 = 2u + 2v$$

Given $a_2 = 6$

$$\therefore 2u + 2v = 6$$

$$u + v = 3 \quad (2)$$

Solving the equations (1) and (2), we get

$$u = 2 \text{ and } v = 1$$

\therefore Explicit formula is $a_n = us_1^n + vs_2^n$

$$= 2(\sqrt{2})^n + (-\sqrt{2})^n$$

Examples:

1. Consider the argument.

All men are fallible.

All kings are men.

\therefore All kings are fallible.

Let $M(x)$ denote the assertion “ x is a man”

$K(x)$ denote the assertion “ x is a king”

$F(x)$ denote the assertion “ x is fallible”

The above argument is symbolised as

$$\begin{array}{l} \forall x, [M(x) \rightarrow F(x)] \\ \forall x, [K(x) \rightarrow M(x)] \\ \hline \therefore \forall x, [K(x) \rightarrow F(x)] \end{array}$$

Proof:

- | | |
|---|-----------------------|
| 1) $\forall x, [M(x) \rightarrow F(x)]$ | Premise 1 |
| 2) $M(c) \rightarrow F(c)$ | Step 1) and Rule 5 |
| 3) $\forall x, [K(x) \rightarrow M(x)]$ | Premise 2 |
| 4) $K(c) \rightarrow M(c)$ | by 3) and Rule 5 |
| 5) $K(c) \rightarrow F(c)$ | by 2) & 4) and Rule 2 |
| 6) $\forall x, [K(x) \rightarrow F(x)]$ | by 5) and Rule 6 |

2. Symbolize the following argument and check for its validity:

Lions are dangerous animals.

There are lions.

∴ There are dangerous animals.

Let $L(x)$ denotes 'x is a lion'

$D(x)$ denotes 'x is dangerous'

Symbolically

$\forall x, [L(x) \rightarrow D(x)]$

$\exists x, L(x)$

∴ $\exists x, D(x)$

Proof:

1. $\forall X, [L(x) \rightarrow D(x)]$ Premise 1
2. $L(c) \rightarrow D(c)$ by 1) and Rule 5
3. $\exists X, L(x).$ Premise 2
4. $L(c)$ by 3) and Rule 7
5. $D(c)$ by 2) & 4) and Rule 1
6. $\exists X, D(x)$ by 5) and Rule 8

Fallacies:

There are three forms of faulty inferences.

1. The **fallacy of affirming the consequent**
(or **affirming the converse**)

$$\begin{array}{l} (p \rightarrow q) \\ q \\ \hline \therefore p \end{array} \quad \text{Fallacy}$$

2. The **fallacy of denying the antecedent**
(or **assuming the opposite**)

$$\begin{array}{l} [(p \rightarrow q) \wedge q] \rightarrow p \text{ is not a tautology} \\ (p \rightarrow q) \\ \sim p \\ \hline \therefore \sim q \end{array} \quad \text{Fallacy}$$

$[(p \rightarrow q) \wedge \sim p] \rightarrow \sim q$ is not a tautology

3. The **non sequitar fallacy**
(means "it does not follow")

$$\begin{array}{l} p \\ \hline \therefore q \end{array}$$

Graph Theory and Applications

- Basic concepts
- Representation of Graphs
- Isomorphism and Sub graphs
- Multi graphs and Euler Circuits
- Hamiltonian graphs
- Spanning trees
- Planar graphs
- Chromatic number

Basic concepts and notations.

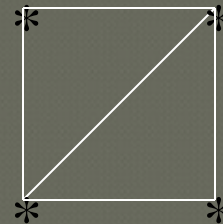
- A **Graph** G is a pair of sets (V, E)
- where $V =$ A set of vertices (nodes) and
- $E =$ A set of edges (lines)
- $V(G) =$ Set of vertices in G .
- $E(G) =$ Set of edges in G .
- $|V(G)| =$ Number of vertices in graph $G =$ Order of G .
- $|E(G)| =$ Number of edges in graph $G =$ Size of G .

a

b

c

d



Types of graphs

- **Non Directed Graph (Undirected graph):** The elements of E are unordered pairs (sets) of vertices. In this case an edge $\{u, v\}$ is said to join u and v or to be between u and v .
- **Directed Graph:** In a *digraph* the elements of E are ordered pairs of vertices. In this case an edge (u, v) is said to be from u to v .
- **Loop:** An edge drawn from a vertex to itself.
- **Multi Graph:** If one allows more than one edge to join a pair of vertices, the result is then called a multi graph.
- **Simple Graph:** A graph with no loops and no parallel edges.
- **Degree:** Degree of a vertex in an undirected graph is the number of edges incident with it, except that a loop at a vertex contributes twice to the degree of that vertex. The degree of the vertex ' v ' is denoted by $\text{deg}(v)$.

Definitions

- **In-degree and Out-degree:** In a digraph, the number of edges incident to a vertex is called the in-degree of the vertex and the number of vertices incident from a vertex is called its out-degree.
- The in-degree of a vertex 'v' in a graph G is denoted by $\deg^+(v)$.
- The out-degree of a vertex v is denoted by $\deg^-(G)$.
- A loop at a vertex in a digraph is counted as one edge for both in-degree and out-degree of that vertex.
- **Neighbors:** If there is an edge incident from u to v, or incident on u and v, then u and v are said to be *adjacent* (neighbors).
- $\delta(G)$ = minimum of all the degrees of vertices in a graph G.
- $\Delta(G)$ = Maximum of all the degrees of vertices in a graph G.

- **Regular Graph:** In a graph G , if $\delta(G) = \Delta(G) = k$ i.e., if each vertex of G has degree k , then G is said to be a regular graph of degree k (k -regular).
- Ex: Polygon is a 2-regular graph .
- Ex: A 3-regular graph is a cubic graph.
- **Complete Graph:** A simple non directed graph with 'n' mutually adjacent vertices is called a complete graph on 'n' vertices and may be represented by K_n .
- **Note:** A complete graph on 'n' vertices has $[\{n(n - 1)\} / 2]$ edges, and each of its vertices has degree 'n-1'.
- Every complete graph is a regular graph.
- The converse of the above statement need not be true.

- **Cycle Graph:** A cycle graph of order 'n' is a connected graph whose edges form a cycle of length n.
- **Note:** A cycle graph ' C_n ' of order n has n vertices and n edges.
- **Null Graph:** A null graph of order n is a graph with n vertices and no edges.
- **Wheel Graph:** A wheel graph of order 'n' is obtained by adding a single new vertex (the hub) to each vertex of a cycle graph of order n.
- **Note:** A wheel graph W_n has 'n + 1' vertices and $2n$ edges.
- **Bipartite Graph:** A Bipartite graph is a non directed graph whose set of vertices can be partitioned in to two sets M and N in such a way that each edge joins a vertex in M to a vertex in N.

More graphs.

- **Complete Bipartite Graph:** A complete Bipartite graph is a Bipartite graph in which every vertex of M is adjacent to every vertex of N .
- If $|M| = m$ and $|N| = n$ then the complete Bipartite graph is denoted by $K_{m,n}$. It has 'm n' edges.
- The number of edges in a bipartite graph is $\leq (n^2/4)$.
- **Degree Sequence:** If v_1, v_2, \dots, v_n are the vertices of a graph G , then the sequence $\{d_1, d_2, \dots, d_n\}$ where $d_i = \text{degree of } v_i$ is called the degree sequence of G .
- Usually we order the degree sequence so that the degree sequence is monotonically decreasing.

First theorem on graph theory

- **Sum of Degrees Theorem:** If $V = \{v_1, v_2, \dots, v_n\}$ is the vertex set of a non directed graph G then
 -
 - $\sum \deg(v_i) = 2 \cdot |E|$
- **Proof:** When the degrees are summed, each edge contributes a count of one to the degree of each of the two vertices on which the edge is incident.
- Hence, the theorem follows.

- Cor. 1 If G is a digraph, then

- $$\sum \deg^+(v_i) = \sum \deg^-(v_i) = |E|$$

- Cor.2. An undirected graph has an even number of vertices of odd degree.
(See Text book for proof)

- Cor.3 If G is a k -regular graph, then $k \cdot |V| = 2 \cdot |E|$.

- Cor.4 In a non directed graph G , If $k = \delta(G)$ and $m = \Delta(G)$ then

- $k \cdot |V| \leq 2 \cdot |E| \leq m \cdot |V|$



Examples

- Ex. A non directed graph contains 16 edges and all vertices are of degree 2.
Find the number of vertices in G ?
- Solution: By Sum of degrees theorem, if degree of each vertex is k, then
- $k \cdot |V| = 2 \cdot |E|$
- $\Rightarrow 2 \cdot |V| = 2 \cdot (16)$
- $\Rightarrow |V| = 16$

Example

- Ex. A simple non directed graph G contains 21 edges, 3 vertices of degree 4 and the other vertices are of degree 2. Find the number of vertices in the graph G ?
- Solution: Let $|V| = n$. By Sum of degrees theorem,
- $\sum \deg(v_i) = 2 \cdot |E|$
- $\Rightarrow 3 \cdot (4) + (n - 3) \cdot 2 = 2 \cdot (21)$
- $\Rightarrow \sum_{i=1}^n 18.$

Ex. What is the number of vertices in an undirected connected graph with 27 edges, 6 vertices of degree 2, 3 vertices of degree 4 and remaining vertices of degree 3?

- ◉ Solution: Let $|V| = n$. By Sum of degrees theorem,
- ◉ $\sum \deg(v_i) = 2 \cdot |E|$
- ◉ $\Rightarrow 6 \cdot (2) + 3 \cdot (4) + (n - 9) \cdot 3 = 2 \cdot (27)$
- ◉ $\Rightarrow n = 19$.

Ex. If a simple non directed graph G contains 24 edges and all vertices are of same degree then find the number of vertices in G ?

- Solution: By Sum of degrees theorem, if degree of each vertex is k , then
- $k \cdot |V| = 2 \cdot |E|$
- $\Rightarrow k \cdot |V| = 2 \cdot (24)$
- $\Rightarrow |V| = 48/k \quad (k = 1, 2, 3, 4, 6, 8, \dots)$
- $|V(G)| = 48, 24, 16, \dots$

Ex. What is the largest possible number of vertices in a graph G , with 35 edges and all vertices are of degree at least 3 ?

- Solution: By Sum of degrees theorem, if degree of each vertex is $\geq k$, then
- $k \cdot |V| \leq 2 \cdot |E|$
- $\Rightarrow 3 \cdot |V| \leq 2 \cdot (35)$
- $\Rightarrow |V| \leq (70/3 = 23.33..)$
- $\Rightarrow |V| \leq 23$
- \therefore The largest possible number of vertices = 23

Example

- Ex. Let G be a simple graph with n vertices. Then show that the number of edges in G is less than or equal to $\{n.(n - 1)\} / 2$.
- Solution: In a simple graph, each edge correspond to a distinct pair of vertices.
- The number of ways to choose a pair of vertices, out of n vertices =
- $$C(n, 2) = \frac{n.(n - 1)}{2}$$
- The maximum number of edges possible in $G = \{n.(n - 1)\} / 2$.
- \therefore The number of edges in G is less than or equal to $\{n.(n - 1)\} / 2$.

Ex. Which of the following degree sequences represent a simple non directed graph

a) $\{2, 3, 3, 4, 4, 5\}$ b) $\{2, 3, 4, 4, 5\}$

c) $\{1, 3, 3, 4, 5, 6, 6\}$ d) $\{1, 3, 3, 3\}$

- Solution: a) Consider the degree sequence $\{2, 3, 3, 4, 4, 5\}$
- Here, we have 3 vertices with odd degree.
- But, By sum of degrees theorem, An undirected graph should contain an even number of vertices of odd degree.
- \therefore The degree sequence cannot represent a simple non directed graph.

- b) Consider the degree sequence $\{2, 3, 4, 4, 5\}$
- Here, we have a vertex with degree 5.
- But, A simple non directed graph of order 5 cannot have a vertex with degree 5.
- \therefore The degree sequence cannot represent a simple non directed graph.

- c) Consider the degree sequence $\{1, 3, 3, 4, 5, 6, 6\}$
Here, the order of the graph is 7 and we have 2 vertices with degree 6.
- Since these two vertices are adjacent to all other vertices of the graph, a vertex with degree 1 does not exist
- \therefore The degree sequence cannot represent a simple non directed graph.

- d) Consider the degree sequence $\{1, 3, 3, 3\}$
Here, the order of the graph is 4 and we have 3 vertices with degree 3.
- Since these 3 vertices are adjacent to all other vertices of the graph, a vertex with degree 1 does not exist.
- \therefore The degree sequence cannot represent a simple non directed graph.

Ex. Show that a degree sequence with all distinct elements cannot represent a simple non directed graph.

- ◉ Solution: Let $G = \{v_1, v_2, v_3, \dots, v_n\}$
- ◉ The possible degree sequences are $\{0, 1, 2, \dots, n-1\}$ and $\{1, 2, 3, \dots, n\}$
- ◉ In a simple graph of order n , if there is a vertex with degree $n-1$ then a vertex with degree 0 does not exist.
- ◉ A simple non directed graph of order ' n ' cannot have a vertex with degree n .
- ◉ \therefore The degree sequence with all distinct elements cannot represent a simple non directed graph.

Havel Hakimi Result

- **Havel Hakimi Result:** Consider the following two sequences and assume the sequence (i) is in descending order
- i) $s, t_1, t_2, \dots, t_s, d_1, d_2, \dots, d_n$
- ii) $t_1 - 1, t_2 - 1, \dots, t_{s-1}, d_1, d_2, \dots, d_n$
- then sequence (i) is graphic iff (ii) is graphic
- Ex. Apply Havel-Hakimi Result to find whether the following degree sequences represent a simple non directed graph.
- $S_1 : \{6, 6, 6, 6, 4, 3, 3, 0\}$
- $S_2 : \{6, 5, 5, 4, 3, 3, 2, 2, 2\}$
- $S_2 : \{1, 1, 3, 3, 3, 4, 6, 7\}$

Representation of Graphs

- Adjacency list: One way to represent a graph with no multiple edges is to use adjacency lists, which specify the vertices that are adjacent to each vertex of the graph.

- **Isomorphic Graphs:** Two graphs G and G^1 are isomorphic if there is a function $f : V(G) \rightarrow V(G^1)$ such that
 - (i) f is a bijection and
 - (ii) for each pair of vertices u and v of G ,
 $\{u, v\} \in E(G) \Leftrightarrow \{f(u), f(v)\} \in E(G^1)$
- i.e.. the function preserves adjacency.
- Note: If G is isomorphic to G^1 then
 - a) $|V(G)| = |V(G^1)|$
 - b) $|E(G)| = |E(G^1)|$
 - c) The degree sequences of G and G^1 are same.
 - d) If $\{v, v\}$ is a cycle in G , then $\{f(v), f(v)\}$ is a loop in G^1 , and more generally, if $v_0 - v_1 - v_2 - \dots - v_k - v_0$ is a cycle of length k in G , then $f(v_0) - f(v_1) - f(v_2) - \dots - f(v_k) - f(v_0)$ is a cycle of length k in G^1 .

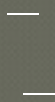
Isomorphism

- Suppose G and G^1 are two graphs and that $f : V(G) \rightarrow V(G^1)$ is a bijection.
- Let A be the adjacency matrix for the vertex ordering v_1, v_2, \dots, v_n of the vertices of G .
- Let A^1 be the adjacency matrix for the vertex ordering $f(v_1), f(v_2), \dots, f(v_n)$ of the vertices of G^1 .
- Then f is an isomorphism from $V(G)$ to $V(G^1)$ iff the adjacency matrices A and A^1 are equal.
- Note: If $A \neq A^1$, then it may still be the case that graphs G and G^1 are isomorphic under some other function.

- **Complement of a graph:** The complement of a graph G is the graph \bar{G} with the same vertices as G . An edge exists in \bar{G} iff it does not exist in G .
- Theorem: Two simple graphs are isomorphic iff their complements are isomorphic.
- If two graphs are isomorphic, then their corresponding sub graphs are isomorphic.
- **Induced Subgraph:** If W is a subset of $V(G)$, then the sub graph induced by W is the sub graph H of G obtained by taking $V(H) = W$ and $E(H)$ to be those edges of G that join pairs of vertices in W .
- If G is isomorphic to \bar{G} then G is said to be self complementary.

Isomorphism

- Ex. If G is self complementary graph with n vertices, then show that
- G has $\{n(n - 1)\}/4$ edges.
- Ex. If G is self complementary then prove that G has $4k$ or $4k + 1$ vertices where k is some positive integer.
- Ex. How many non isomorphic graphs are there of order 4 and size 2?
- Ex. How many non isomorphic graphs are there of order 8, size 8 and degree sequence $\{2,2,2,2,2,2,2,2\}$.
- Ex. How many non isomorphic graphs are there of order 6, size 6 and degree sequence $\{2, 2, 2, 2, 2, 2\}$.
- Ex. Let C_n be a cycle graph on n vertices. if C_n is isomorphic to C_n then show that $n = 5$.



Euler Path and Circuit

- **Euler Path:** An Euler path in a multi graph is a path that includes each edge of the multi graph exactly once and intersects each vertex of the multi graph at least once.
- An **Euler circuit** is an Euler path whose end points are identical.
- A multi graph is traversable if it has Euler path.
- A non directed multi graph has an Euler path iff it is connected and has zero or exactly two vertices of odd degree.
- Any finite connected graph with exactly two odd vertices is traversable(Euler path exists). A traversable trail may begin at either odd vertex and will end at other odd vertex.
- A connected multi graph has an *Euler circuit* if and only if all of its vertices are of even degree.

Hamiltonian Graph

- **Hamiltonian Graph:** A Hamiltonian Graph is a graph with a closed path that includes every vertex exactly once. Such a path is a cycle and is called a Hamiltonian cycle.
- An Eulerian circuit uses every edge exactly once but may repeat vertices , while a Hamiltonian cycle uses each vertex exactly once (except for the first and last) but may skip edges.

Spanning Trees

- Tree: A connected graph with no cycles is called a tree.
- A tree with 'n' vertices has $(n - 1)$ edges.
- A tree with n vertices ($n > 1$) has at least two vertices of degree 1.
- A sub graph H of a graph G is called a spanning tree of G if
 - i) H is a tree and
 - ii) H contains all vertices of G
- Note: In general, if G is a connected graph with n vertices and m edges, a spanning tree of G must have $(n - 1)$ edges. Therefore, the number of edges that must be removed before a spanning tree is obtained must be $m - (n - 1)$. This number is called *circuit rank* of G.
- A non directed graph G is connected iff G contains a spanning tree.
- The complete graph K_n has n^{n-2} different spanning trees.

(Caley's formula)

- Breadth first search : (Algorithm for finding a spanning tree of a connected graph)
- The idea of BFS is to visit all vertices sequentially on a given level before going to next level.
- **Input:** A connected graph G.
- **Output:** A spanning tree for G.
- Method:
- (Refer Text book by Mott, Kandell and Baker)

- Depth first search : (Algorithm for finding a spanning tree of a connected graph)
- The idea of DFS is proceeding to higher levels successively in the first opportunity. Later we backtrack and add the vertices which are not visited.
- **Input:** A connected graph G.
- **Output:** A spanning tree for G.
- Method:
- (Refer Text book by Mott, Kandell and Baker)

Minimal Spanning Tree: Let G be a connected graph where each edge of G is labeled with a non negative cost. A spanning tree T where the total cost $C(T)$ is minimum is called a minimal spanning tree.

- **Kruskal's Algorithm:** (For finding minimal spanning tree of a connected weighted graph)
- **Input:** A connected graph G with non negative values assigned to each edge.
- **Output:** A minimal spanning tree for G .
- **Method:** 1) Select any edge of minimal value that is not a loop. This is the first edge of T (if there is more than one edge of minimal value, arbitrary choose one of these edges)
- 2) Select any remaining edge of G of having minimal value that does not form a circuit with the edges already included in T .
- 3) Continue step 2 until T contain $(n - 1)$ edges when $n = |V(G)|$

Prim's algorithm.

- **Prim's Algorithm:** (For finding a minimal spanning tree)
- 1) Let G be a connected graph with non negative values assigned to each edge. First let T be the tree consisting of any vertex V_1 of G .
- 2) Among all the edges not in T , that are incident on a vertex in T and do not form a circuit when added to T , Select one of minimal cost and add it to T .
- 3) The process terminates after we have added $(n - 1)$ edges
- where $n = |V(G)|$.
-

Planar Graphs

- A graph or a multi graph that can be drawn in a plane or on a sphere so that its edges do not cross is called a **planer graph**.
- Ex : A complete graph on 4 vertices K_4 is a planar graph.
- Ex : Tree is a planar graph.
- **Map, Connected map** : A particular planar representation of a finite planer multi graph is called a map. We say that the map is connected if the underlying multi graph is connected.
- **Region** : A given map (planar graph) divide the plane into connected areas called regions
- **Degree of a region** : The boundary of each region of a map consists of a sequence of edges forming a closed path. The degree of region 'r' denoted by $\text{deg}(r)$ is the length of the closed path bordering r .

Sum of degrees of regions theorem

- If G is a planar graph with k regions, then the sum of the degrees of the regions of G is equal to twice the number of edges in G .
i.e., $\sum \deg(r_i) = 2 \cdot |E|$.
- Cor.1 In a planar graph G , if the degree of each region is k then
 $k \cdot |R| = 2 \cdot |E|$
- Cor.2 In a planar graph G , if the degree of each region is $\geq k$, then
 $k \cdot |R| \leq 2 \cdot |E|$
- In particular, If G is a simple connected planar graph (A planar graph with no loops and no parallel edges, and degree of each region is ≥ 3), then
 $3 \cdot |R| \leq 2 \cdot |E|$

Euler's formula

- ◉ Question: State and prove Euler's formula for planar graphs.
- ◉ Statement: If G is a connected planar graph, then
- ◉ $|V| - |E| + |R| = 2$.
- ◉ Proof:
- ◉ Theorem: If G is a simple connected planar graph with $|E| > 1$ then,
 - (a) $|E| \leq \{3 \cdot |V| - 6\}$.
 - (b) There exists at least one vertex v of G such that $\deg(v) \leq 5$
- ◉ Proof:
- ◉ Theorem: If G is a simple connected planar graph with $|V| > 3$ then,
 - $|R| \leq \{2 \cdot |V| - 4\}$.

Polyhedral graph

- **Polyhedral Graph:** A connected plane graph is said to be polyhedral if degree of each region is ≥ 3 and $\deg(v) \geq 3$ for all $v \in G$.
i.e., $3 \cdot |R| \leq 2 \cdot |E|$ and $3 \cdot |V| \leq 2 \cdot |E|$.

- For any polyhedral graph

- a) $|V| \geq (2 + |R|)$

- b) $|R| \geq (2 + \frac{|V|}{2})$

- c) $(3 \cdot |R| - 6) \geq |E|$ —
—

Kurtowski Theorem

- A graph G is not planar iff G contains a sub graph homeomorphic to $K_{3,3}$ or K_5 .
- Ex. A planar graph contains 25 vertices and 60 edges then find the number of regions in the graph.
- Ex. What is the maximum number of edges possible in a planar graph with eight vertices?
- Ex. What is the minimum number of vertices necessary for a graph with 11 edges to be a simple planar graph?
- Ex. Suppose that a connected planar graph has 20 vertices, each of degree 3. In to how many regions does a representation of this planar graph split the plane?

Examples

- Ex. Let G is a connected planar graph with 35 regions and degree of each region is 6. Find the number of vertices in G ?
- Ex. Suppose G is a polyhedral graph with 12 vertices and 30 edges prove that degree of each region is 3.
- Ex. Show that there does not exist a polyhedral graph with exactly seven edges.
- Ex. Show that there does not exist a polyhedral graph with exactly 30 edges and 11 regions.
- Theorem: Prove that a complete graph K_n is planar iff $n \leq 4$.
- Theorem: Prove that a complete Bipartite graph $K_{m,n}$ is planar
iff $m \leq 2$ or $n \leq 2$.

- **Vertex coloring:** A coloring of a simple graph is the assignment of color to each vertex of the graph so that no two adjacent vertices are assigned the same color.
- **Chromatic Number:** The minimum number of colors needed to paint a graph G is called the chromatic number of G , denoted by $\chi(G)$
- **Adjacent Regions:** In a planar graph two regions are adjacent if they share a common vertex.
- **Map coloring:** An assignment of colors to the regions of a map such that adjacent regions have different colors.
- A map 'M' is n – colorable if there exists a coloring of M which uses n colors.
- A planar graph is 5 – colorable

Four color Theorem

- **Four color Theorem:** If the regions of a planar graph are colored so that adjacent regions have different colors, then no more than 4 colors are required.
i.e., $\chi(G) \leq 4$.
- Ex. Prove that the chromatic number of a complete graph K_n is n .
- Ex. Prove that the chromatic number of a complete Bipartite graph $K_{m,n}$ is 2.
- Ex. Prove that the chromatic number of cyclic graph C_n is 2 if n is even and 3 if n is odd.
- Ex. If every cycle of G has even length then show that its chromatic number is 2.
- Ex. Prove that the chromatic number of a tree on n vertices is 2.