What is discrete mathematics?

- Discrete mathematics is the branch of mathematics dealing with objects that can assume only **distinct, separated values**.
- The term "discrete mathematics" is therefore used in contrast with "continuous mathematics," which is the branch of mathematics dealing with objects that can vary smoothly (and which includes, for example, calculus)
- It is used in programming languages, software development, cryptography, algorithms etc.
- Discrete Mathematics covers some important concepts such as set theory, graph theory, logic, permutation and combination as well.

Example:

- Determine in how many ways can three gifts be shared among 4 boys in the following conditions-

No one gets more than one gift.

Solution:

The first gift can be given in 4 ways as one cannot get more than one gift, the remaining two gifts can be given in 3 and 2 ways respectively.

The total number of ways = 4 x 3 x 2 = 24.

Examples…

Kinds of problems solved using discrete mathematics include:

1. How many ways are there to choose a valid password on a computer system?
2. What is the probability of winning a lottery?
3. Is there a link between two computers in a network?
4. How can I identify spam e-mail messages?
5. How can I encrypt a message so that no unintended recipient can read it?
6. What is the shortest path between two cities using a transportation system?

Continued….

- How can a list of integers be sorted so that the integers are in increasing order?
- How many steps are required to do such a sorting?
- How can it be proved that a sorting algorithm correctly sorts a list?
- How can a circuit that adds two integers be designed?
- How many valid Internet addresses are there?

Discrete mathematics covers:

- Set Theory
- Permutation and Combination
- Graph Theory
- Logic
- Sequence and Series

First, through this course you can develop your mathematical maturity: that is, your ability to understand and create mathematical arguments.

Discrete mathematics provides the mathematical foundations for many computer science courses including data structures, algorithms, database theory, automata theory, formal languages, compiler theory, computer security, and operating systems.

Logic

- The rules of logic give precise meaning to mathematical statements.
- It helps us to understand and reason about different mathematical statement.
- We would be able to prove or disprove those statement precisely.
- Purpose of logic is to create a valid arguments or proof.
- Once it is proved TRUE, it is called theorem.

Example…

- “For every positive integer n, the sum of the positive integers not exceeding n is n(n + 1)/2.”
- This statement can be either valid or FALSE.
- With the help rules of logic, we can reason it and come to conclusion that it is valid argument.

Proposition

- A proposition is a **declarative** sentence (that is, a sentence that **declares a fact**) that is either true or false, but not both.
- All the following declarative sentences are propositions.

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

- Propositions 1 and 3 are true,
- Propositions 2 and 4 are false.

Continued…

- Consider the following sentences.

1. What time is it?
2. Read this carefully.
3. $x + 1 = 2$.
4. $x + y = z$.

- Sentences 1 and 2 are not propositions because they are not declarative sentences.
- Sentences 3 and 4 are not propositions because they are neither true nor false.
- Note that each of sentences 3 and 4 can be turned into a proposition if we assign values to the variables

Variables

- We use variable to denote proposition.
- Conventional letters used for propositional variables are p, q, r, s, ... The truth value of a proposition is true, denoted by T, if it is a true proposition, and the truth value of a proposition is false, denoted by F, if it is a false proposition.
- The area of logic that deals with propositions is called the **propositional calculus** or **propositional logic**.
- A **proposition** is simply a statement. **Propositional logic** studies the ways statements can interact with each other.

Combining/ modifying proposition

1. Negation: Let p be a proposition. The negation of p, denoted by **¬p** (also denoted by $\overline{p}$), is the statement "It is not the case that p."

   for example: p: Michael's PC runs Linux

- Negation of above statement is : **¬p :**"It is not the case that Michael's PC runs Linux."
- This negation can be more simply expressed as

  "Michael's PC does not run Linux."

p	**¬p**
T	F
F	T

Example…

- Find the negation of the proposition

p: “Vandana’s smartphone has at least 32GB of memory” .

- Solution: The negation is **¬p :**“It is not the case that Vandana’s smartphone has at least 32GB of memory.”
- This negation can also be expressed as **¬p :**“Vandana’s smartphone does not have at least 32GB of memory”
- or even more simply as **¬p :** “Vandana’s smartphone has less than 32GB of memory.”

Conjunction(continued…)

- Let p and q be propositions.
- The conjunction of p and q, denoted by **p ∧ q**, is the proposition "**p and q**." The conjunction p ∧ q is true when both p and q are true and is false otherwise.
- If p: the sun is shinning, q: it is raining.
- Then **p ∧ q :** the sun is shinning and it is raining.
- For this conjunction to be true, both conditions

given must be true. It is false, when one or both of

these conditions are false.

p	**q**	**p ∧ q**
F	F	F
F	T	F
T	F	F
T	T	T

- It Is like AND operation.

Disjunction

- Let p and q be propositions.
- The disjunction of p and q, denoted by **p V q**, is the proposition "**p or q**." The disjunction p V q is false when both p and q are false and is true otherwise.
- Students who have taken calculus **or** computer science can take this class.
- Here, we mean that students who have taken both calculus and computer science can take the class, as well as the students who have taken only one of the two subjects.
- Also sometime referred as inclusive OR.

p	q	p V q
F	F	F
F	T	T
T	F	T
T	T	T

Exclusive OR

- Let p and q be propositions. The exclusive or of p and q, denoted by **$p \oplus q$**, is the proposition that is true when exactly one of p and q is true and is false otherwise.
- Consider the statement: in order to get job in this company, c++ or java experience but not both is mandatory.
- You get job if you have experience in c++.

  If you have experience in java. If experience in both, you don't get.
- What about this???
  - Soup or salad comes free with this food item.

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

Implication

- Let p and q be propositions. The conditional statement p → q is the proposition "if p, then q."
- In the conditional statement p → q, **p is called the hypothesis** (or antecedent or premise) and **q is called the conclusion** (or consequence).
- Note that the statement p → q is true when both p and q are true and when p is false, it Is always true no matter what truth value q has.

p	q	p → q
F	F	T
F	T	T
T	F	F
T	T	T

Implication example..

- “If you get 100% marks on final exam, then you will get award”

Case i: p: you got 100%, q:you got award.

true

Case ii: p: you got 100%, q:you didn’t get award.

false

Case iii: p: you didn’t get 100%, q:you got award.

true.

Case iv: p: you didn’t get 100%, q:you didn’t get award.

true.

Trick or approach.....

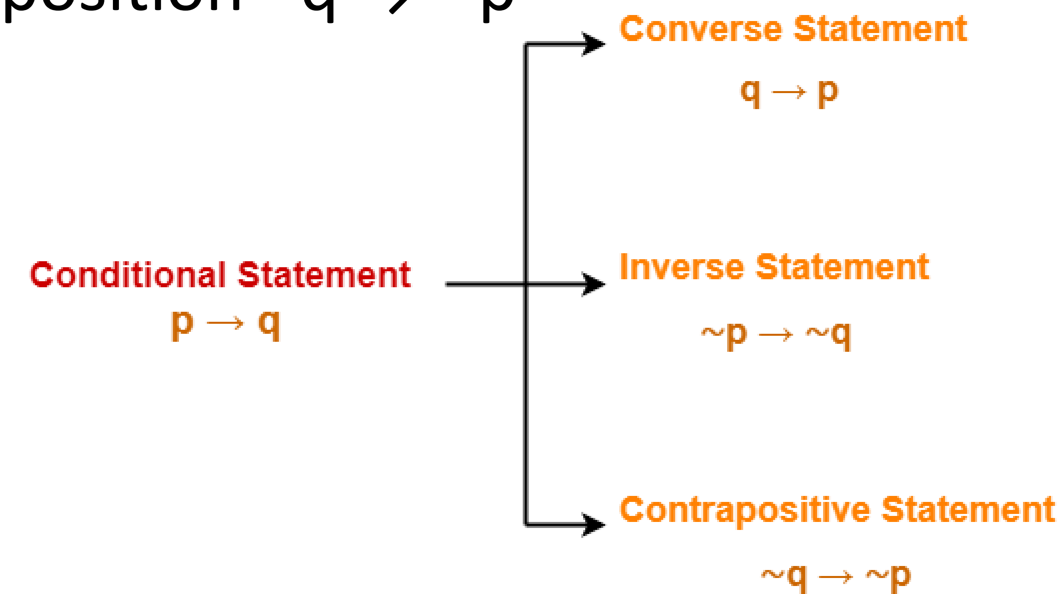
- If I guessed RIGHT then answered RIGHT, it make sense(it is RIGHT)
- If I guessed RIGHT then answered WRONG, it doesn't make sense (it is WRONG)
- If I guessed WRONG then answered RIGHT, it still make sense (It is RIGHT)
- If I guessed WRONG then answered WRONG, it still make sense (It is RIGHT)

Representation of implication

- "if p, then q"
- "p implies q"
- "if p, q"
- "p is sufficient for q"
- "a sufficient condition for q is p"
- "q if p"
- "q whenever p"
- "q when p"
- "q is necessary for p"
- "p only if q"
- "a necessary condition for p is q"
- "q follows from p"
- "q unless ¬p"

Converse ,inverse and contrapositive

- We can form some new conditional statements starting with a conditional statement $p \rightarrow q$.
- The proposition $q \rightarrow p$ is called the converse of $p \rightarrow q$
- The proposition $\neg p \rightarrow \neg q$ is called the inverse of $p \rightarrow q$
- The contrapositive of $p \rightarrow q$ is the proposition $\neg q \rightarrow \neg p$



Contd…..

- Converse statement ($q \rightarrow p$) and inverse statement ($\sim p \rightarrow \sim q$) are equivalent to each other.
- $p \rightarrow q$ and its contrapositive statement ($\sim q \rightarrow \sim p$) are equivalent to each other.
- Example:
- $p \rightarrow q$:If today is Sunday, then it is a holiday.

  p: today is Sunday

  q: it is a holiday

Contd…..

- **Converse Statement-** If it is a holiday, then today is Sunday.
- **Inverse Statement-** If today is not Sunday, then it is not a holiday.
- **Contrapositive Statement-** If it is not a holiday, then today is not Sunday.

2. "If it rains, then I will stay at home."

- **Converse Statement-** If I will stay at home, then it rains.
- **Inverse Statement-** If it does not rain, then I will not stay at home.
- **Contrapositive Statement-** If I will not stay at home, then it does not rain.

Finding logical equivalency

- Let the conditional statement be “if a polygon is a square, then it also a quadrilateral.”
- Converse: “if it is a quadrilateral, then it is a square.”
- Think whether it is true or false?
- It may or mayn’t be square.
- Inverse: “if polygon isn’t square, then it also not quadrilateral.”
- What about this?
- Only square is not a quadrilateral.

Biconditional

- Let p and q be propositions. The biconditional statement **$p \leftrightarrow q$** is the proposition “p if and only if q.” **The biconditional statement $p \leftrightarrow q$ is true when p and q have the same truth values**, and is false otherwise.
- Biconditional statements are also called bi-implications.
- p if and only if q is composed of two sentence.
- “p if q” and “p only if q”.
- “p only if q” is equivalent to “if p then q”. Also “p if q” is equivalent to “if q then p”.
- Therefore it represent biconditional statement.

Contd…

- . There are some other common ways to express $p \leftrightarrow q$:
  - “p is necessary and sufficient for q”
  - “if p then q, and conversely”
  - “p iff q.”

p	**q**	**$p \leftrightarrow q$**
F	F	T
F	T	F
T	F	F
T	T	T

Truth table of compound proposition

- To construct the truth table of compound proposition, we need to know the precedence of different operator.

Operator	Precedence
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

Example…

- Construct the truth table of the compound proposition

  $(p \lor \neg q) \rightarrow (p \land q)$.

p	q	$\neg q$	$p \lor \neg q$	$p \land q$	$(p \lor \neg q) \rightarrow (p \land q)$
T	T	F	T	T	T
T	F	T	T	F	F
F	T	F	F	F	T
F	F	T	T	F	F

Application of proposition logic

- Logic has many important applications to mathematics, computer science, and numerous other disciplines.
- Propositional logic and its rules can be used to design computer circuits, to construct computer programs, to verify the correctness of programs, and to build expert systems.
- Some of the application are:
  - Translating English Sentences
  - System Specifications
  - Boolean Searches
  - Logic Puzzles
  - Logic Circuits

Translating English sentence

- Reason to translate English sentence into logical expression.
- To remove ambiguity.
- For eg:
- I have never tasted a cake quite like that one before!
- Ambiguity: Was the cake good or bad?
- Did you see her dress?
- Ambiguity: Is she getting dressed or are they talking about her clothes?

Practice

- Q.1 “You can access the Internet from campus if you are a computer science major or you are not a freshman.”
- Solution:
- Steps:
- check for all possible proposition.
- Check for logical connectives in English form.
- Write proposition in positive term.
- Put them all logically.

Contd…

- P: you are a computer science major
- Q: you are a freshman
- R: You can access the Internet from campus
- $(p \vee \sim q) \rightarrow r$
- Q2. “if I go to movie or the store, I won’t do my homework”
- P: I go to movie.
- Q: I go to the store.
- R: I do my homework.
- $(p \vee q) \rightarrow \sim r$

Contd…

- “You cannot ride the roller coaster if you are under 4 feet tall unless you are older than 16 years old.”
- Let q: “You can ride the roller coaster,”
- r: “You are under 4 feet tall”, and
- S: “You are older than 16 years old,”
- Then
- $(r \wedge \neg s) \rightarrow \neg q$.

System specification

- Consistent system specifications do not contain conflicting requirements that could be used to derive a contradiction.
- When specifications are not consistent, there is no way to develop a system that satisfies all the specifications.
- To determine consistency, first translate the specifications into logical expressions; then determine whether any of the specifications conflict with one another.

Example…

- The system is in multiuser state if and only if it is operating normally.
- If the system is operating normally, the kernel is functioning.
- The kernel is not functioning or the system is in interrupt mode.
- If the system is not in multiuser state, then it is in interrupt mode.
- The system is not in interrupt mode.

Solution

Let p: The system is in multiuser state

q: it is operating normally

Contd…

- r: the kernel is functioning
- s: system is in interrupt mode
- Now, $p \longleftrightarrow q$, $q \rightarrow r$, $\sim r \vee s$, $\sim p \rightarrow s$, $\sim s$.
- s need to be false for ~s to be true.
- ~p should be false for $\sim p \rightarrow s$ to be true.
- ~r need to be true for $\sim r \vee s$ to be true.(r is false)
- q should be false for $q \rightarrow r$ to be true.
- p is also false if q is false for biconditional. Overall it is false.
- Not consistent.

Contd…

- Determine whether these system specifications are consistent: “The diagnostic message is stored in the buffer or it is retransmitted.” “The diagnostic message is not stored in the buffer.” “If the diagnostic message is stored in the buffer, then it is retransmitted.”
- Solution:
- To determine whether these specifications are consistent, we first express them using logical expressions. Let p denote “The diagnostic message is stored in the buffer”
- q denote “The diagnostic message is retransmitted.”
- The specifications can then be written as $p \lor q$, $\neg p$, and $p \rightarrow q$.
- An assignment of truth values that makes all three specifications true must have p false to make $\neg p$ true.

Contd…

- Because we want $p \vee q$ to be true but p must be false, q must be true.
- Because $p \rightarrow q$ is true when p is false and q is true, we conclude that these specifications are consistent, because they are all true when p is false and q is true.

Logical puzzle…

- In an island that has two kinds of inhabitants, **knights**, who always tell the truth, and their opposites, **knaves**, who always lie. You encounter two people A and B. What are A and B if A says “B is a knight” and B says “The two of us are opposite types?”

Solution:

Let p: “A is a knight”

q: “B is a knight”

Contd…

p	q	A says about B i.e B is a knight	B says we are opposite types $(\sim p \wedge q) \vee (p \wedge \sim q)$	remarks
T	T	T	F	contradiction
T	F	F	T	Not valid
F	T	T	T	Not valid
F	F	F	F	valid

Therefore both are knave from above truth table

Muddy children puzzle…

- A father tells his two children, a boy and a girl, to play in their backyard without getting dirty. However, while playing, both children get mud on their foreheads. When the children stop playing, the father says “At least one of you has a muddy forehead,” and then asks the children to answer “Yes” or “No” to the question: “Do you know whether you have a muddy forehead?” The father asks this question twice. What will the children answer each time this question is asked, assuming that a child can see whether his or her sibling has a muddy forehead, but cannot see his or her own forehead? Assume that both children are honest and that the children answer each question simultaneously.

Contd….

- Let s : “son has a muddy forehead” and d: “daughter has a muddy forehead.”

s	d	s˅d
T	T	T
T	F	T
F	T	T
F	F	F(not valid)

First time both will answer no as they are in doubt whether they have or not

Second time both will answer yes as they know each other condition

MUDDY HEAD PUZZLE

CASE 1

Son will say 'No'
Because he is in Doubt as mother said at least one of them have muddy head

Daughter will also say 'No'
Because she is also Doubt as mother said at least one of them have muddy head

---

CASE 2

Son will say 'Yes'
Because now he knows the answer of his sister.

Daughter will also say 'Yes'
Because she also knows the answer of his brother

The Lady or the Tiger Puzzle

- Two door leads to different room. Each room contain either lady or tiger. The goal is to locate the lady. In this puzzle truth table of two door match. Room 1 has written “at least one of this room contain lady” and room 2 has written “the tiger is in other room”.

Solution:

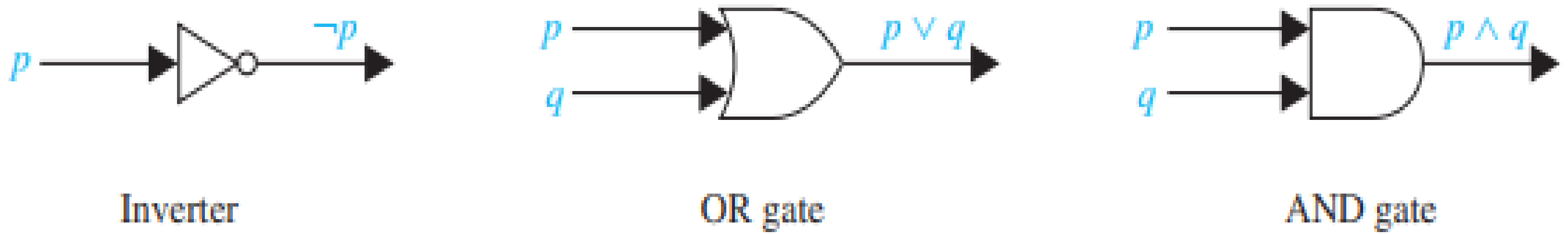
Let p: “room 1 contain lady” and q: “room 2 contain lady.”

Contd…

P	q	Room 1 says p$\vee$ q	Room 2 says ~p	remarks
T	T	T	F	X
T	F	T	F	X
F	T	T	T	Valid
F	F	F	T	X

Logic circuits.

- Propositional logic can be applied to the design of computer hardware.
- A logic circuit (or digital circuit) receives input signals p1, p2,...,pn, each a bit [either 0 (off) or 1 (on)], and produces output signals s1, s2,...,sn, each a bit.

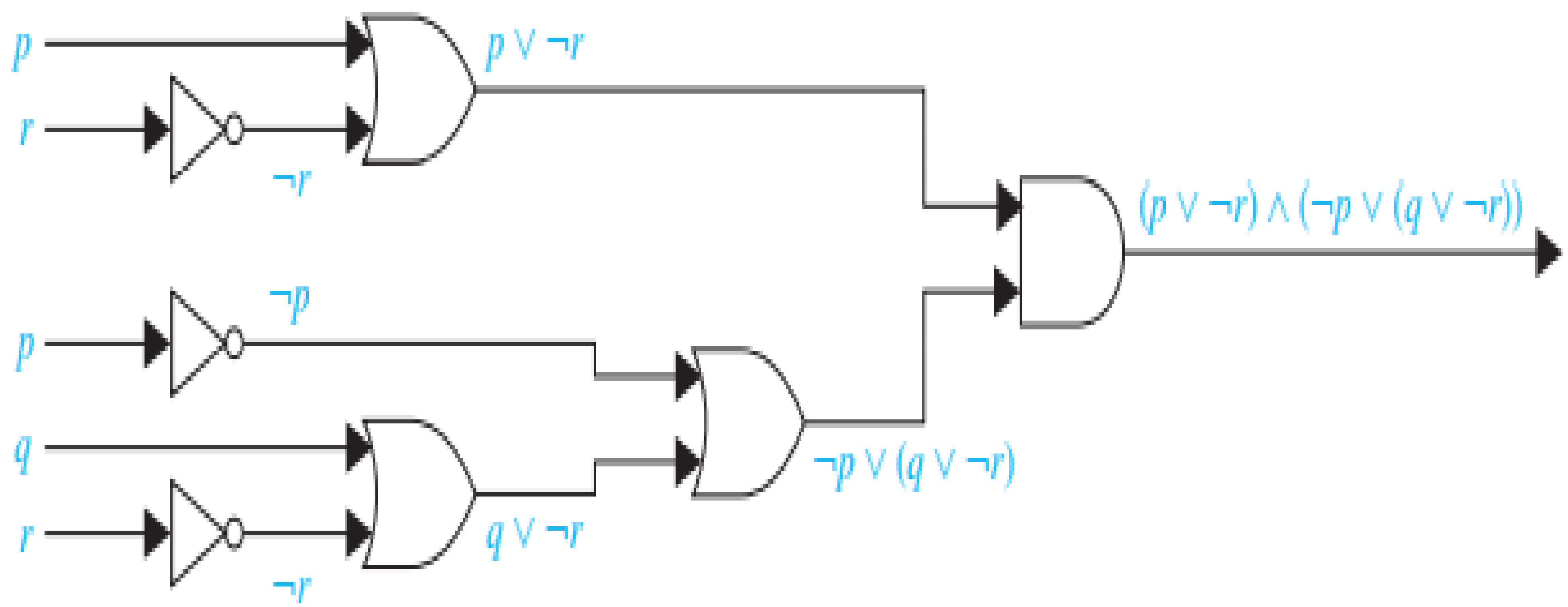


Basic logic gates

Cntd…

- Complicated digital circuits can be constructed from three basic circuits, called gates.
- The inverter, or NOT gate, takes an input bit p, and produces as output $\neg p$.
- The OR gate takes two input signals p and q, each a bit, and produces as output the signal $p \vee q$.
- Finally, the AND gate takes two input signals p and q, each a bit, and produces as output the signal $p \wedge q$.
- We use combinations of these three basic gates to build more complicated circuits,

Q. Build a digital circuit that produces the output $(p \lor \neg r) \land (\neg p \lor (q \lor \neg r))$ when given input bits p, q, and r.



Propositional equivalences

- **Tautology** : compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it.
- **Contradiction**: A compound proposition that is always false.
- **Contingency**: A compound proposition that is neither a tautology nor a contradiction i.e. sometime true and sometime false.
- Tautologies and contradictions are often important in mathematical reasoning.

Contd…

P	~p	P ˅ ~P
T	F	T
F	T	T

Tautology

P	~p	P ^ ~P
T	F	F
F	T	F

contradiction

P	q	P ^ q
T	T	T
T	F	F
F	T	F
F	F	F

contingency

Satisfiability and unsatisfiability

- A compound proposition is satisfiable if there is at least one truth result in its table.
- Tautology is always satisfiable.
- If there is no single truth result in its table, then it is unsatisfiable.
- Contradiction is always unsatisfiable.
- A compound proposition is **valid** if it is tautology.
- If it is contradiction or contingency, then it is **invalid**.

Logical equivalence..

- The compound propositions p and q are called logically equivalent if p $\leftrightarrow$ q is a tautology.
- The notation p ≡ q denotes that p and q are logically equivalent.
- The symbol ⇔ is sometimes used instead of ≡ to denote logical equivalence.
- One of the way to check whether logically equivalent or not is by construction of truth table.

Show that $p \to q$ and $\neg p \vee q$ are logically equivalent.

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

Logical equivalence

Equivalence	*Name*
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws

$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws

De- Morgan’s law of propositional logic

- Logical equivalences known as De Morgan’s laws are particularly important.
- They tell us how to negate conjunctions and how to negate disjunctions.
- Two laws are:
  1. $\neg(p \lor q) \equiv \neg p \land \neg q$
  2. $\neg(p \land q) \equiv \neg p \lor \neg q$

Use De Morgan's laws to express the negations of "Miguel has a cellphone and he has a laptop computer"

- Let p be "Miguel has a cellphone" and q be "Miguel has a laptop computer."
- Then "Miguel has a cellphone and he has a laptop computer" can be represented by $p \wedge q$.
- By the first of De Morgan's laws, $\neg(p \wedge q)$ is equivalent to $\neg p \vee \neg q$.
- Consequently, we can express the negation of our original statement as "Miguel does not have a cellphone or he does not have a laptop computer."

Predicates

- Consider the statement
- “If today is Saturday, there wont be class”
- “Today is Saturday”
- therefore “There wont be class”
- Consider the next statement
- “Students of this class are talent”
- “shyam is a student”
- Therefore “shyam is talent”

Contd..

- **Predicates** are the statement involving variables that are either true or false unless the value of variable are specified.
- For eg: “x = y + 3”; it is not proposition.
- The statement “**x is greater than 3**” has two parts. The first part, the variable x, is the **subject** of the statement.
- The second part—the **predicate**, “is greater than 3”—refers to a property that the subject of the statement can have.
- We can denote the statement “x is greater than 3” by **P (x),** where P denotes the predicate “is greater than 3” and x is the variable(subject).

Contd…

- Let P (x) denote the statement “x > 3.” What are the truth values of P (4) and P (2)?
- For P(4) i.e 4>3 it is True
- For P(2) i.e 2>3 it is false
- Let A(x) denote the statement “Computer x is under attack by an intruder.” Suppose that of the computers on campus, only CS2 and MATH1 are currently under attack by intruders. What are truth values of A(CS1), A(CS2), and A(MATH1)?

Quantifiers

- When the variables in a propositional function are assigned values, the resulting statement becomes a proposition with a certain truth value.
- Quantification expresses **the extent** to which a predicate is true over a **range of elements**.
- In English, the words all, some, many, none, and few are used in quantifications instead of numbers.

Types of quantifier..

- Universal quantifier

- It tells us that a predicate is **True** for every element under consideration(domain).
- The domain must always be specified when a universal quantifier is used.
- The universal quantification of P (x) is the statement "P (x) for all values of x in the domain."
- The notation ∀x P (x) is used which is read as **"for all x P (x)" or "for every x P (x)."**

Contd..

- Let P (x) be the statement “$x + 1 > x$.” What is the truth value of the quantification $\forall x\, P(x)$, where the domain consists of all real numbers?
- Because P (x) is true for all real numbers x, the quantification $\forall x\, P(x)$ is true.
- Besides “for all” and “for every,” universal quantification can be expressed in many other ways, including “all of,” “for each,” “given any,” “for arbitrary,” “for each,” and “for any.”

Contd…

- Let $Q(x)$ be the statement "$x < 2$." What is the truth value of the quantification $\forall x\, Q(x)$, where the domain consists of all real numbers?
- Solution: $Q(x)$ is not true for every real number x, because, for instance, $Q(3)$ is false.
- That is, $x = 3$ is a **counterexample** for the statement $\forall x\, Q(x)$. Thus $\forall x\, Q(x)$ is false.
- Note that a single counterexample is all we need to establish that $\forall x\, P(x)$ is false

Types contd…

- Existential Quantifier

- It is true if and only if P (x) is true for at least one value of x in the domain.
- The existential quantification of P (x) is the proposition “There exists an element x in the domain such that P (x).”
- We use the notation $\exists x\, P(x)$ for the existential quantification of P (x).
- $\exists x\, P(x)$ is read “For some x P (x).”
- Some other phrase “for some,” “for at least one,” or “there is” can be used.

Contd…

- Let P (x) denote the statement "$x > 3$." What is the truth value of the quantification $\exists x\, P(x)$, where the domain consists of all real numbers?
- Solution: Because "$x > 3$" is sometimes true—for instance, when $x = 4$—the existential quantification of P (x), which is $\exists x\, P(x)$, is true.
- Let Q(x) denote the statement "$x = x + 1$." What is the truth value of the quantification $\exists x\, Q(x)$, where the domain consists of all real numbers?
- Solution: Because Q(x) is false for every real number x, the existential quantification of Q(x), which is $\exists x\, Q(x)$, is false.

Quantifiers with restricted domain

- What do the statements ∀x < 0 (x^2 > 0), and ∃z > 0 (z^2 = 2) mean, where the domain in each case consists of the real numbers?
- The statement ∀x < 0 (x2 > 0)states that for every real number x with x < 0, x2 > 0.
- That is, it states “The square of a negative real number is positive.”
- This statement is the same as ∀x(x < 0 → x^2 > 0).
- the statement ∃z > 0 (z^2 = 2) states that there exists a real number z with z > 0 such that z^2 = 2.
- That is, it states “There is a positive square root of 2.” This statement is equivalent to ∃z(z > 0 ∧ z^2 = 2).

Logical equivalence involving quantifiers.

- Two logical statements involving predicates and quantifiers are considered equivalent if and only if they have the same truth value no matter which predicates are substituted into these statements irrespective of the domain used for the variables in the propositions
- Two important equivalence are

$$\forall x(P(x) \land Q(x)) \equiv \forall x P(x) \land \forall x Q(x)$$

$$\exists x(P(x) \lor Q(x)) \equiv \exists x P(x) \lor \exists x Q(x)$$

Negating quantified expression

- Let us consider the statement “Every student in your class has taken a course in discrete structures.”
- The negation of above statement is “It is not the case that every student in your class has taken a course in discrete structures.”
- “There is a student in your class who has not taken a course in discrete structures” is also equivalent.
- Thus we can obtain following relation $\neg\forall x\, P(x) \equiv \exists x\, \neg P(x)$.

Contd…

- Suppose we wish to negate an existential quantification.
- For instance, consider the proposition “There is a student in this class who has taken a course in calculus.”
- This is the existential quantification $\exists x\ Q(x)$.
- The negation of this statement is the proposition “It is not the case that there is a student in this class who has taken a course in calculus.”
- This is equivalent to “Every student in this class has not taken calculus.”
- $\neg\exists x\ Q(x) \equiv \forall x\ \neg Q(x)$ holds true.

What are the negations of the statements “All Americans eat cheeseburgers”?

- Let $C(x)$ denote “x eats cheeseburgers.”
- Then the statement “All Americans eat cheeseburgers” is represented by $\forall x\, C(x)$, where the domain consists of all Americans.
- The negation of this statement is $\neg \forall x\, C(x)$, which is equivalent to $\exists x\, \neg C(x)$.
- This negation can be expressed in several different ways, including “Some American does not eat cheeseburgers” and “There is an American who does not eat cheeseburgers.”

English to logical equation

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

Solution:

Let us consider domain for above statement to be every student in the class.

we introduce a variable x so that our statement becomes “For every student x in this class, x has studied calculus.”

we introduce C(x), which is the statement “x has studied calculus.”

we can translate our statement as $\forall x\, C(x)$.

Contd…

- For example, we may be interested in a wider group of people than only those in this class.
- If we change the domain to consist of all people, we will need to express our statement as “For every person x, if person x is a student in this class then x has studied calculus.”
- If S(x) represents the statement that person x is in this class, we see that our statement can be expressed as $\forall x\,(S(x) \rightarrow C(x))$.
- Our statement cannot be expressed as $\forall x(S(x) \wedge C(x))$ because this statement says that all people are students in this class and have studied calculus.

Nested quantifier…

- Two quantifiers are said to be nested if one is within the scope of another.
- $\forall x\ \exists y\ Q(x , y)$; $\exists$ is within the scope of $\forall$.
- Note that everything within the scope of a quantifier can be thought of as a propositional function.
- For example, $\forall x\ \exists y(x + y = 0)$ is the same thing as $\forall x\ Q(x)$, where $Q(x)$ is $\exists y\ P (x, y)$, where $P (x, y)$ is $x + y = 0$.

Contd…

- Translate into English the statement $\forall x \, \forall y((x > 0) \wedge (y < 0) \rightarrow (x\,y < 0))$, where the domain for both variables consists of all real numbers. Solution:
- This statement says that for every real number x and for every real number y, if $x > 0$ and $y < 0$, then $x\,y < 0$.
- That is, this statement says that for real numbers x and y, if x is positive and y is negative, then x y is negative.
- This can be stated as “The product of a positive real number and a negative real number is always a negative real number.”

Contd…

- Let $Q(x, y)$ denote “$x + y = 0$.” What are the truth values of the quantifications $\exists y \forall x\, Q(x, y)$ and $\forall x \exists y\, Q(x, y)$, where the domain for all variables consists of all real numbers?
- The quantification $\exists y \forall x\, Q(x, y)$ denotes the proposition “There is a real number y such that for every real number x, $Q(x, y)$.”
- No matter what value of y is chosen, there is only one value of x for which $x + y = 0$. Because there is no real number y such that $x + y = 0$ for all real numbers x, the statement $\exists y \forall x\, Q(x, y)$ is false.
- The quantification $\forall x \exists y\, Q(x, y)$ denotes the proposition “For every real number x there is a real number y such that $Q(x, y)$.” Given a real number x, there is a real number y such that $x + y = 0$; namely, $y = -x$. Hence, the statement $\forall x \exists y\, Q(x, y)$ is true.

Translate the statement “The sum of two positive integers is always positive” into a logical expression.

- $\forall x\ \forall y((x > 0) \wedge (y > 0) \rightarrow (x + y > 0))$
- Here the domain is all real numbers for x and y with restricted domain positive integer for both x and y.
- this can also be written as $\forall x\ \forall y(x + y > 0)$, where the domain for both variables consists of all positive integers.

Translate the statement "Every real number except zero has a multiplicative inverse."

- We first rewrite this as "For every real number x except zero, x has a multiplicative inverse."
- We can rewrite this as "For every real number x, if $x = 0$, then there exists a real number y such that $x\,y = 1$."
- This can be rewritten as $\forall x((x = 0) \rightarrow \exists y(x\,y = 1))$.
- Note: practice more from kenth rosen book pg. 62 example 11 onwards.

Rules of inference

- Basic terminology:
- Premise: it is proposition on the basis of which we can draw the conclusion. It can be said as arguments or evidence.
- Conclusion: it is proposition which can be reached from set of premise. It is result of assumption.
- Arguments: a sequence of statements(arguments) that end with a conclusion.
- Valid arguments: an argument is valid if and only if it is impossible for all the premises to be true and the conclusion to be false.

Example…

- Consider the following argument involving propositions (which, by definition, is a sequence of propositions):
- “If you have a current password, then you can log onto the network.”
- $P \rightarrow q$
- “You have a current password.”
- p
- Therefore, “You can log onto the network.”
- $\therefore q$
- From the definition of a valid argument form we see that the argument form with premises $p1, p2,...,pn$ and conclusion q is valid, when $(p1 \land p2 \land \cdots \land pn) \rightarrow q$ is a tautology.

Contd…

- Rules of Inference provide the templates or guidelines for constructing valid arguments from the statements that we already have.
- To deduce new statements from the statements whose truth that we already know, **Rules of Inference** are used.
- Generating the conclusions from evidence and facts is termed as **Inference**.

Types of rules of inference

1. Modus ponens or law of detachment:

- modus ponens tells us that if a conditional statement and the hypothesis of this conditional statement are both true, then the conclusion must also be true.
- Using this notation, the hypotheses are

written in a column, followed by a

horizontal bar, followed by a line that

begins with the therefore symbol and ends with the conclusion.

$$\begin{array}{rl} & p \\ & p \to q \\ \hline \therefore & q \end{array}$$

Example…

- Determine whether the argument given here is valid and determine whether its conclusion must be true because of the validity of the argument. If $\sqrt{2} > \frac{3}{2}$ $then$ $\left(\sqrt{2}\right)^2 > \left(\frac{3}{2}\right)^2$
- Let p: $\sqrt{2} > \frac{3}{2}$ and q: $\left(\sqrt{2}\right)^2 > \left(\frac{3}{2}\right)^2$
- Premises are p→ q, p and conclusion q.
- As one of its argument i.e p is false the conclusion is also false.

Rule of Inference	*Tautology*	*Name*
p $p \to q$ $\therefore q$	$(p \land (p \to q)) \to q$	Modus ponens
$\neg q$ $p \to q$ $\therefore \neg p$	$(\neg q \land (p \to q)) \to \neg p$	Modus tollens
$p \to q$ $q \to r$ $\therefore p \to r$	$((p \to q) \land (q \to r)) \to (p \to r)$	Hypothetical syllogism
$p \lor q$ $\neg p$ $\therefore q$	$((p \lor q) \land \neg p) \to q$	Disjunctive syllogism
p $\therefore p \lor q$	$p \to (p \lor q)$	Addition
$p \land q$ $\therefore p$	$(p \land q) \to p$	Simplification
p q $\therefore p \land q$	$((p) \land (q)) \to (p \land q)$	Conjunction
$p \lor q$ $\neg p \lor r$ $\therefore q \lor r$	$((p \lor q) \land (\neg p \lor r)) \to (q \lor r)$	Resolution

Rules of inference

State which rule of inference is used in the argument:

- If it rains today, then we will not have a barbecue today. If we do not have a barbecue today, then we will have a barbecue tomorrow. Therefore, if it rains today, then we will have a barbecue tomorrow.
- Let p be the proposition “It is raining today,” let q be the proposition “We will not have a barbecue today,” and let r be the proposition “We will have a barbecue tomorrow.”
- Then this argument is of the form $p \rightarrow q$
- $q \rightarrow r$
- $\therefore p \rightarrow r$
- Hence, this argument is a hypothetical syllogism

Building arguments…

- Show that the premises “It is not sunny this afternoon and it is colder than yesterday,” “We will go swimming only if it is sunny,” “If we do not go swimming, then we will take a canoe trip,” and “If we take a canoe trip, then we will be home by sunset” lead to the conclusion “We will be home by sunset.”
- Let p :“It is sunny this afternoon,”
- q :“It is colder than yesterday,”
- r :“We will go swimming,”
- s :“We will take a canoe trip,” and
- t :“We will be home by sunset.”

Contd…

- Then the premises become $\neg p \land q$, $r \rightarrow p$, $\neg r \rightarrow s$, and $s \rightarrow t$. The conclusion is simply t.

steps	arguments	reason
1	$\neg p \land q$	premise
2	$\neg p$	Simplification on 1
3	$r \rightarrow p$	premise
4	$\neg r$	Modus tollens on 2 and 3
5	$\neg r \rightarrow s$	premise
6	s	Modus ponens on 4 and 5
7	$s \rightarrow t$	premise
8	t	Modus ponens on 6 and 7

Sample question…

- “If it does not rain or if is not foggy, then the sailing race will be held and the lifesaving demonstration will go on. If the sailing race is held, then the trophy will be awarded. The trophy was not awarded.” implies “It rained”
- Show that the premises “If you send me an e-mail message, then I will finish writing the program,” “If you do not send me an e-mail message, then I will go to sleep early,” and “If I go to sleep early, then I will wake up feeling refreshed” lead to the conclusion “If I do not finish writing the program, then I will wake up feeling refreshed.”

Is the following argument valid?

- If you do every problem in this book, then you will learn discrete mathematics. You learned discrete mathematics. Therefore, you did every problem in this book.
- Let p be the proposition “You did every problem in this book.” Let q be the proposition “You learned discrete mathematics.” Then this argument is of the form: if $p \rightarrow q$ and q, then p.
- This is an example of an incorrect argument using the fallacy of affirming the conclusion. Indeed, it is possible for you to learn discrete mathematics in some way other than by doing every problem in this book.
- It is invalid.

fallacies

- Argument which at first seems to be right but are invalid is known as fallacy.
- P $\rightarrow$ q, q, therefore p.
- When p is false and q is true, the conclusion is false. Therefore p is not logical consequence of P $\rightarrow$ q and q.
- The above argument is called as fallacy of affirming the conclusion.

Example..

- If today is Tuesday, then there will be discrete structure class.($p \rightarrow q$)
- There is discrete structure class. (q)
- Therefore today is Tuesday. (p)
- There is no logical consequence of p from $p \rightarrow q$ and q.

Rules of inference for quantified statement

Rule of Inference	*Name*
$\dfrac{\forall x\, P(x)}{\therefore\; P(c)}$	Universal instantiation
$\dfrac{P(c) \text{ for an arbitrary } c}{\therefore\; \forall x\, P(x)}$	Universal generalization
$\dfrac{\exists x\, P(x)}{\therefore\; P(c) \text{ for some element } c}$	Existential instantiation
$\dfrac{P(c) \text{ for some element } c}{\therefore\; \exists x\, P(x)}$	Existential generalization

Types

- **Universal instantiation** is the rule of inference used to conclude that P (c) is true, where c is a particular member of the domain, given the premise ∀x P (x).
- **Universal generalization** is the rule of inference that states that ∀x P (x) is true, given the premise that P (c) is true for all elements c in the domain.
- **Existential instantiation** is the rule that allows us to conclude that there is an element c in the domain for which P (c) is true if we know that ∃x P (x) is true. Here c cannot be arbitrary.

Contd…

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

Example…

- Show that the premises “A student in this class has not read the book,” and “Everyone in this class passed the first exam” imply the conclusion “Someone who passed the first exam has not read the book.”
- Let $C(x)$ be “x is in this class,”
- $B(x)$ be “x has read the book,” and
- $P(x)$ be “x passed the first exam.”
- Premises are $\exists x(C(x) \land \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$.

Contd..

Step	Reason
1. $\exists x(C(x) \land \neg B(x))$	Premise
2. $C(a) \land \neg B(a)$	Existential instantiation from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x(C(x) \to P(x))$	Premise
5. $C(a) \to P(a)$	Universal instantiation from (4)
6. $P(a)$	Modus ponens from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \land \neg B(a)$	Conjunction from (6) and (7)
9. $\exists x(P(x) \land \neg B(x))$	Existential generalization from (8)

Universal modus ponens

- Universal instantiation and modus ponens are often used together, this combination of rules is sometimes called **universal modus ponens.**
- $\forall x(P(x) \rightarrow Q(x))$
- $P(a)$, where a is a particular element in the domain

- $\therefore Q(a)$
- Universal modus ponens is commonly used in mathematical arguments.

Example….

- Assume that “For all positive integers n, if n is greater than 4, then n^2 is less than 2^n” is true. Use universal modus ponens to show that $100^2 < 2^{100}$.
- Let P (x) denote “x is greater than 4” and Q(x) denote “square of x is less than 2^x”
- The statement “For all positive integers x, if x is greater than 4, then x^2 is less than 2^x” can be represented by
- ∀x(P (x) → Q(x)), where the domain consists of all positive integers.

Contd…

- We are assuming that $\forall x(P(x) \rightarrow Q(x))$ is true.
- Note that $P(100)$ is true because $100 > 4$.
- It follows by universal modus ponens that $Q(100)$ is true, namely that $100^2 < 2^{100}$.
- In summary,
- $\forall x(P(x) \rightarrow Q(x))$,
- $P(100)$
- $\therefore Q(100)$

Introduction to proof

- A proof is a valid argument that establishes the truth of a mathematical statement.
- A proof can use the hypotheses of the theorem, if any, axioms assumed to be true, and previously proven theorem.
- Using these ingredients and rules of inference, the final step of the proof establishes the truth of the statement being proved.

Terminology

1. **Theorem** is a statement that can be shown to be true. It is usually reserved for a statement that is considered at least somewhat important.
2. **Proof** is a valid argument that establishes the truth of a theorem.
3. **Axioms (postulates) :** The statements used in a proof which are statements we assume to be true.
4. **Lemma is** less important theorem that is helpful in the proof of other results. They are used in understanding of complicated proof.

Contd…

5. **Corollary** is a theorem that can be established directly from a theorem that has been proved.
6. **Conjecture** is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert.

   When a proof of a conjecture is found, the conjecture becomes a theorem. Many times conjectures are shown to be false, so they are not theorems.

Direct proof

- In a direct proof of a conditional statement $p \to q$ we first assume that p is true.
- Subsequent steps are constructed using rules of inference, axioms, previously proven theorem with the final step showing that q must also be true.
- The integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k such that $n = 2k + 1$

Give a direct proof of the theorem “If n is an odd integer, then n^2 is odd.”

- By the definition of an odd integer, it follows that n = 2k + 1, where k is some integer.
- We can square both sides of the equation n = 2k + 1
- n^2 = $(2k + 1)^2$= $4k^2$ + 4k + 1 = 2($2k^2$ + 2k) + 1= 2(r)+1.
- By the definition of an odd integer, we can conclude that n^2 is an odd integer.

Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square.

- An integer a is a perfect square if there is an integer b such that a = b^2.
- We assume n= s^2 and m= t^2 to be true.
- For nm = $s^2\ t^2$ = (ss) (tt)= (st)(st) =$(st)^2$ where s, t are both integer.

Q. Give a direct proof that sum of two even integer is even.

Proof by contraposition.

- Direct proofs lead from the premises of a theorem to the conclusion.
- In indirect proof we do not start with the premises and end with the conclusion.
- The conditional statement $p \to q$ can be proved by showing that its contrapositive, $\neg q \to \neg p$, is true.
- we take $\neg q$ as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that $\neg p$ must follow true.

Prove that if n is an integer and 3n + 2 is odd, then n is odd.

- It is in the form of “ if 3n+2 is odd, then n is odd”. P$\rightarrow$ q.
- By contraposition ~q $\rightarrow$ ~p
- We start with n is even.
- Then, by the definition of an even integer, n = 2k for some integer k.
- 3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1).
- It follows that 3n+2 is also even as it is multiple of 2.

Proof by contradiction

- It is also one type of indirect proof.
- We start by assuming a proposition is not “TRUE”.
- We find contradiction such that proposition was “TRUE”.

Q. Prove that square root of 2 is irrational by proof by contradiction.

Solution:

Here p: $\sqrt{2}$ is irrational.

Let us assume ~p i.e. $\sqrt{2}$ is rational.

Contd…

- We can write $\sqrt{2} = \frac{a}{b}$; b $\neq 0$ and a and b has no common factor.
- Squaring both sides $2 = \frac{a^2}{b^2}$ or $2b^2 = a^2$
- Therefore a is even
- $2b^2 = (2c)^2$ or $2b^2 = 4c^2$ or $b^2 = 2c^2$
- Therefore b is also even.
- Now $\frac{a}{b}$ has common factor 2.
- Therefore $\sqrt{2}$ is irrational.

Q. Give a proof by contradiction of the theorem "If $3n + 2$ is odd, then n is odd."

- Let p be "$3n + 2$ is odd" and q be "n is odd." To construct a proof by contradiction, assume that both p and $\neg q$ are true.
- That is, assume that $3n + 2$ is odd and that n is not odd. Because n is not odd, we know that it is even.
- Because n is even, there is an integer k such that $n = 2k$. This implies that $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$.
- Because $3n + 2$ is $2t$, where $t = 3k + 1$, $3n + 2$ is even.
- Note that the statement "$3n + 2$ is even" is equivalent to the statement $\neg p$, because an integer is even if and only if it is not odd. Because both p and $\neg p$ are true, we have a contradiction.
- This completes the proof by contradiction, proving that if $3n + 2$ is odd, then n is odd.

Mistakes in proof

- There are many common errors made in constructing mathematical proofs.
- Each step of a mathematical proof needs to be correct and the conclusion needs to follow logically from the steps that precede it.
- Many mistakes result from the introduction of steps that do not logically follow from those that precede it

What is wrong with this famous supposed "proof" that 1 = 2?

- We use these steps, where a and b are two equal positive integers.

Step	**Reason**
1. $a = b$	Given
2. $a^2 = ab$	Multiply both sides of (1) by a
3. $a^2 - b^2 = ab - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Factor both sides of (3)
5. $a + b = b$	Divide both sides of (4) by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$ and simplify
7. $2 = 1$	Divide both sides of (6) by b

Mathematical induction

- Mathematical induction is like climbing a infinite ladder.
- In this type of induction two statement always follow
  - 1. We can reach the first rung of the ladder.
  - 2. If we can reach a particular rung of the ladder, then we can reach the next rung.
- It is used to prove results about the complexity of algorithms, the correctness of certain types of computer programs, theorems about graphs and trees, as well as a wide range of identities and inequalities.

Contd…

- Mathematical induction is based on the rule of inference that tells us that if $P(1)$ and $\forall k(P(k) \to P(k+1))$ are true for the domain of positive integers, then $\forall n\, P(n)$is true.
- Understanding how to read and construct proofs by mathematical induction is a key goal of learning discrete mathematics.
- To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:
- BASIS STEP: We verify that $P(1)$ is true. Where 1 is the first element of positive integer.
- INDUCTIVE STEP: We show that the conditional statement $P(k) \to P(k+1)$ is true for all positive integers k.

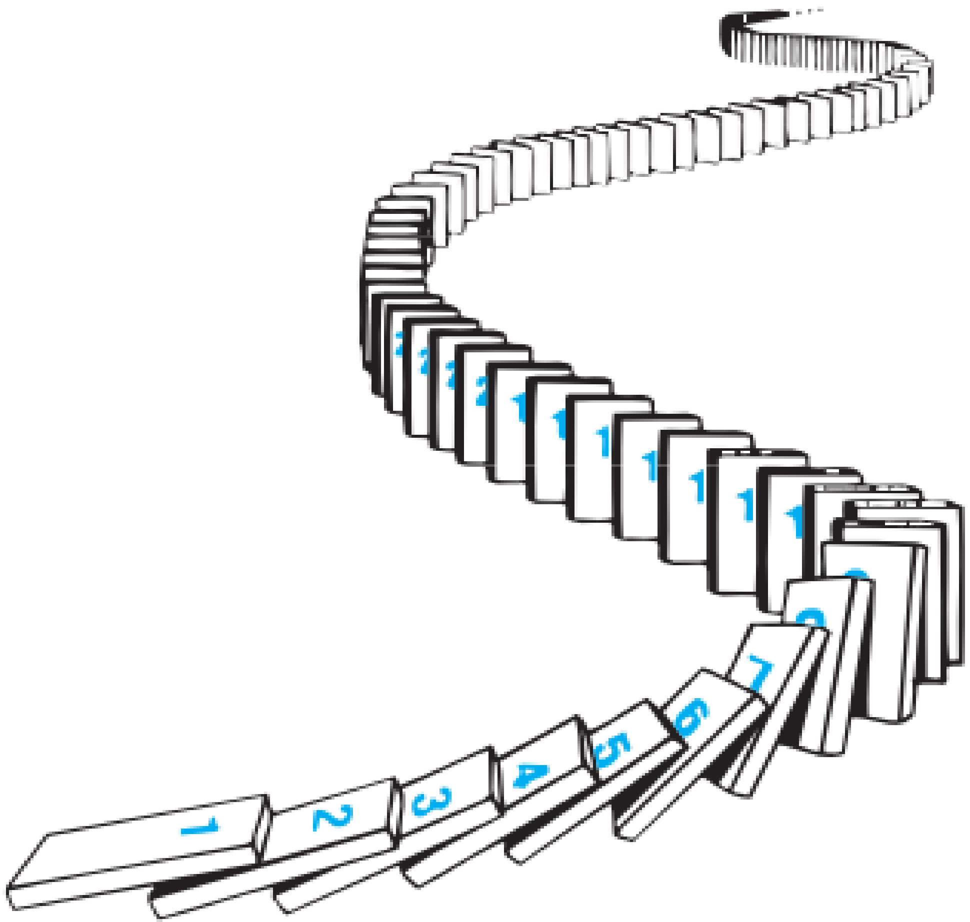


Illustration of working of mathematical induction

Proving summation formula

- Show that if n is a positive integer, then $1 + 2 + \cdots + n = n(n + 1)/2$.
- Let $P(n)$ be the proposition that the sum of the first n positive integers, $1 + 2 + \cdots n = n(n+1)\ 2$, is $n(n + 1)/2$.
- BASIS STEP: $P(1)$ is true, because $1 = 1(1 + 1)/2$ or 1=1(T).
- INDUCTIVE STEP: For the inductive hypothesis we assume that $P(k)$ holds for an arbitrary positive integer k. That is, we assume that

$1 + 2 + \cdots + k = k(k + 1)/2$.

it must be shown that $P(k + 1)$ is true, namely, that $1 + 2 + \cdots + k + (k + 1) = (k + 1)[(k + 1) + 1]/2 = (k + 1)(k + 2)/2$

Contd..

- $1 + 2 + \cdots + k + (k + 1) = k(k + 1)/ 2 + (k + 1) = k(k + 1) + 2(k + 1) 2 = (k + 1)(k + 2) /2$.
- We have completed the basis step and the inductive step, so by mathematical induction we know that P (n) is true for all positive integers n. That is, we have proven that $1 + 2 + \cdots + n = n(n + 1)/2$ for all positive integers n.

Use mathematical induction to show that $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ for all nonnegative integers n.

- Let P (n) be the proposition that $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ for the integer n.
- BASIS STEP: P (0) is true because $2^0 = 2^{0+1} - 1$ or 1=1(T)
- INDUCTIVE STEP: For the inductive hypothesis, we assume that P (k) is true for an arbitrary nonnegative integer k.
- $1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$
- we must show that $1 + 2 + 2^2 + \cdots + 2^k + 2^{k+1} = 2^{k+2} - 1$
- $1 + 2 + 2^2 + \cdots + 2^k + 2^{k+1} = 2^{k+1} - 1 + 2^{k+1} = 2^{k+2} - 1$

Conjecture a formula for the sum of the first n positive odd integers. Then prove your conjecture using mathematical induction.

Use mathematical induction to prove the inequality n < 2^n for all positive integers n.

- Let P (n) be the proposition that n < 2n.
- BASIS STEP: P (1) is true, because 1 < 2^1 = 2. This completes the basis step.
- INDUCTIVE STEP: P(k)is the statement that k < 2^k
- we need to show that if P (k) is true, then P (k + 1), which is the statement that k + 1 < 2^{k+1}, is true.
- k + 1 < $2^k + 1 <$ 2^k+ 2^k $<$ 2 ⋅ 2^k = 2^{k+1}

Use mathematical induction to prove that 2^n < n! for every integer n with n ≥ 4.

- Let P (n) be the proposition that 2^n < n!
- BASIS STEP: P (4), 16 < 24 is true.
- INDUCTIVE STEP: For the inductive step, we assume that P (k)is true for an arbitrary integer k with k ≥ 4.
- we must show that if 2^k< k! for an arbitrary positive integer k where k ≥ 4, then 2^{k+1} < (k + 1)!
- 2^k. 2< 2 · k! or $2^{k+1} < (k+1).k!$ Or 2^{k+1}<(k+1)!.

Use mathematical induction to prove that $7^{n+2} + 8^{2n+1}$ is divisible by 57 for every nonnegative integer n.

- To construct the proof, let P (n) denote the proposition: “$7^{n+2} + 8^{2n+1}$ is divisible by 57.”
- BASIS STEP: To complete the basis step, we must show that P (0) is true. $7^{0+2} + 8^{2*0+1}$=49+8=57/57 (T).
- Inductive hypothesis: we assume that $7^{k+2} + 8^{2k+1}$ is divisible by 57.
- we must show that when we assume that the inductive hypothesis P (k) is true, then P (k + 1), the statement that $7^{k+3} + 8^{2k+3}$ is divisible by 57, is also true.

Contd..

- 7(k+1)+2 + 82(k+1)+1 = 7k+3 + 82k+3 = 7 · 7k+2 + 82 · 82k+1 = 7 · 7k+2 + 64 · 82k+1 = 7(7k+2 + 82k+1) + 57 · 82k+1.

Strong induction and well ordering

- It is another form of mathematical induction, called strong induction, which can often be used when we cannot easily prove a result using mathematical induction.
- The basis step of a proof by strong induction is the same as a proof of the same result using mathematical induction.
- However, the inductive steps in these two proof methods are different.

Contd…

- STRONG INDUCTION To prove that P (n) is true for all positive integers n, where P (n) is a propositional function, we complete two steps:
- BASIS STEP: We verify that the proposition P (1) is true.
- INDUCTIVE STEP: We show that the conditional statement $[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$ is true for all positive integers k.
- Note that when we use strong induction to prove that P (n) is true for all positive integers n, our inductive hypothesis is the assumption that P (j) is true for j = 1, 2,...,k. That is, the inductive hypothesis includes all k statements P (1), P (2), . . . , P (k).

Show that if n is an integer greater than 1, then n can be written as the product of primes.

- Let P (n) be the proposition that n can be written as the product of primes.
- BASIS STEP: P (2) is true, because 2 can be written as the product of one prime, itself.
- INDUCTIVE STEP: The inductive hypothesis is the assumption that P (j) is true for all integers j with $2 \leq j \leq k$, that is, the assumption that j can be written as the product of primes whenever j is a positive integer at least 2 and not exceeding k.

Contd…

- We must be show that $P(k + 1)$ is true under this assumption, that is, that $k + 1$ is the product of primes.
- There are two cases to consider, namely, when $k + 1$ is prime and when $k + 1$ is composite.
- If $k + 1$ is prime, we immediately see that $P(k + 1)$ is true.
- Otherwise, $k + 1$ is composite and can be written as the product of two positive integers a and b with $2 \leq a \leq b<k+1$.
- Because both a and b are integers at least 2 and not exceeding k, we can use the inductive hypothesis to write both a and b as the product of primes. Thus, if $k + 1$ is composite.

Semantic tableau(pl. tableaux)

- Since the 1980s, alternative techniques for determining argument validity on PCs or LPCs have gained popularity both because of their ease of learning and their ease of implementation by computer programs.
- Based on the observation that the premises of a valid argument cannot be true while the conclusion is false, this method interprets the premises so that they are all simultaneously satisfied, even if the conclusion is negated.
- Success in such an effort would show the argument to be invalid, while failure to find such an interpretation would show it to be valid.

Contd..

- Basic idea is an inference is valid if and only if there exist no counter example such that premise holds true and conclusion is false.

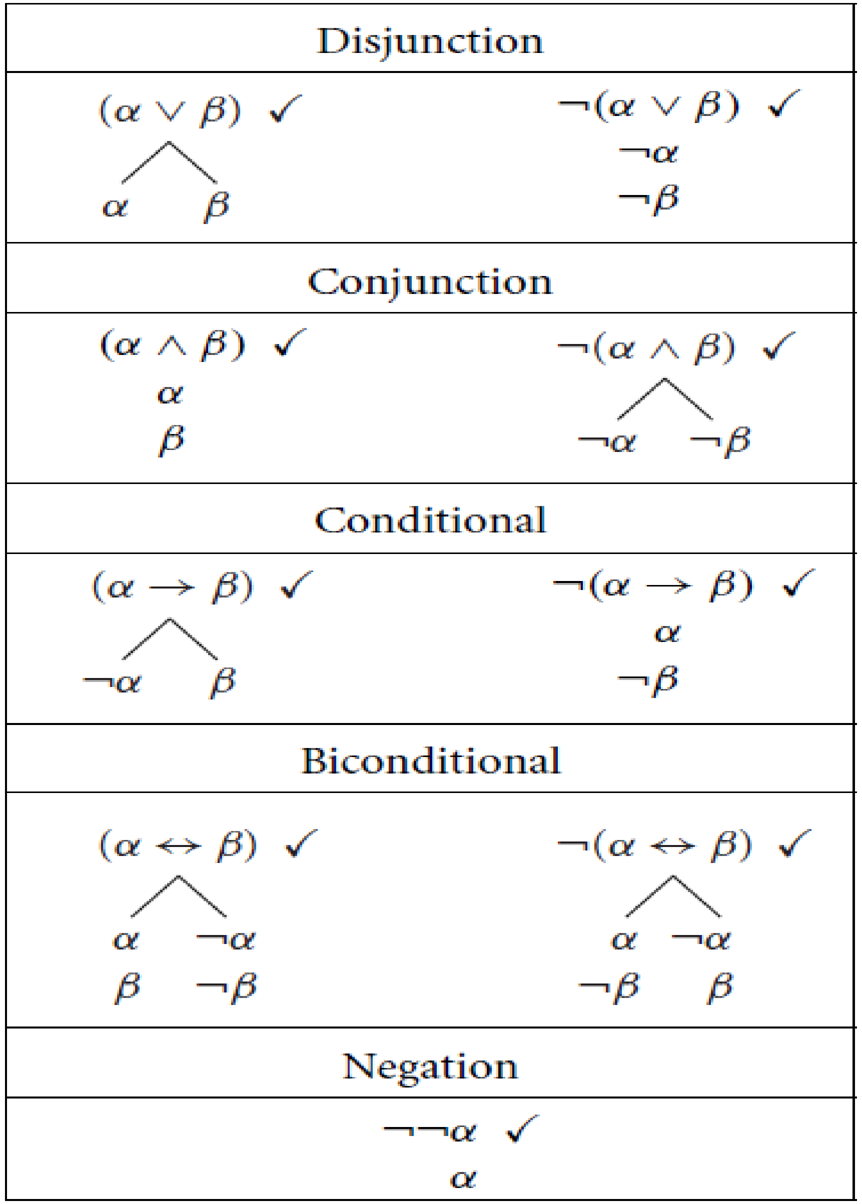


Figure 7.1. Tree rules for PL.

Some practice problem..

- See the class problem…