Unit 4: Logic, Induction and Reasoning

Contents Overview

- 4.1 Propositions and Truth Functions
- 4.2 Propositional Logic
- 4.3 Propositional Equivalences
- 4.4 Predicate logic and Quantifiers
- 4.5 Deduction in Predicate logic
- 4.6 Rules of Inferences
- 4.7 Mathematical Reasoning- Direct Proof and Indirect Proof (Proof by Contradiction and Proof By Contraposition)
- 4.8 Mathematical Induction

PROPOSITIONS AND TRUTH FUNCTIONS, PROPOSITIONAL LOGIC

Logic

- Crucial for mathematical reasoning
- Important for program design
- Used for designing electronic circuitry

- (Propositional)Logic is a system based on propositions.
- A proposition is a (declarative) statement that is either true or false (not both).
- We say that the truth value of a proposition is either true (T) or false (F).
- Corresponds to 1 and 0 in digital circuits

The Statement/Proposition Game

"Elephants are bigger than mice."

Is this a statement? yes

Is this a proposition? yes

What is the truth value of the proposition? true

The Statement/Proposition Game

"$520 < 111$"

Is this a statement?	yes
Is this a proposition?	yes
What is the truth value of the proposition?	false

The Statement/Proposition Game

"$y > 5$"

Is this a statement? yes

Is this a proposition? no

Its truth value depends on the value of y, but this value is not specified.

We call this type of statement a propositional function or open sentence.

The Statement/Proposition Game

"Today is January 27 and $99 < 5$."

Is this a statement? yes

Is this a proposition? yes

What is the truth value of the proposition? false

The Statement/Proposition Game

- "Please do not fall asleep."

Is this a statement? no

It's a request.

Is this a proposition? no

Only statements can be propositions.

The Statement/Proposition Game

- “x < y if and only if y > x.”

Is this a statement? yes

Is this a proposition? yes

… because its truth value does not depend on specific values of x and y.

What is the truth value of the proposition? true

Terms

- We use letters such as p,q,r,.. to denote propositional variables or statement variables
- The truth value of proposition is denoted by T if it is true and denoted by F if it is false.
- The area that deals with propositions is called propositional calculus or propositional logic
- New propositions, called compound propositions are formed from existing propositions using logical operators

Logical Operators (Connectives)

- We will examine the following logical operators:

- Negation (NOT, $\neg$)
- Conjunction (AND, $\wedge$)
- Disjunction (OR, $\vee$)
- Exclusive-or (XOR, $\oplus$)
- Implication (if – then, $\rightarrow$)
- Biconditional (if and only if, $\leftrightarrow$)

- Truth tables can be used to show how these operators can combine propositions to compound propositions.

Negation (NOT)

- Unary Operator, Symbol: $\neg$

p	$\neg p$
true (T)	false (F)
false (F)	true (T)

$\wedge$

Let p be propositions. The negation of p is statement that “ It is not the case that p”

Conjunction (AND)

- Binary Operator, Symbol: $\wedge$

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

Today is Friday (p) . It is raining today (q).
Conjunction is Today is Friday and it is raining today

Let p and q be propositions. The conjunction or of p and q is proposition that is true when both of p and q is true and is false otherwise

Disjunction (OR)

- Binary Operator, Symbol: $\vee$

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

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

Let p and q be propositions. The disjunction or of p and q is proposition that is false when both p and q is false and is true otherwise

Exclusive Or (XOR)

- Binary Operator, Symbol: $\oplus$

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

Let p and q be propositions. The exclusive or of p and q is proposition that is true when exactly one of p and q is true and is false otherwise

Conditional statement: Implication (if - then)

- Binary Operator, Symbol: $\rightarrow$

p	q	p→q
T	T	T
T	F	F
F	T	T
F	F	T

If p then q
P implies q
P is sufficient for q
p only if

Eg: If I am elected, I will lower taxes
If you get 100%, you will get A

Let p and q be propositions. The conditional statement $\mathbf{p \rightarrow q}$ is proposition "if p then q". The statement is false when p is true and q is false and true otherwise. Here p is hypothesis and q is conclusion.

Biconditional (if and only if)

- Binary Operator, Symbol: $\leftrightarrow$

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

Biconditional (if and only if)

- Binary Operator, Symbol: $\leftrightarrow$

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

Biconditional (if and only if)

- Binary Operator, Symbol: $\leftrightarrow$

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

Biconditional (if and only if) XNOR

- Binary Operator, Symbol: $\leftrightarrow$

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

Let p and q be propositions. The conditional statement **$p \leftrightarrow q$** is proposition "p if and only if q". The statement is true when both statements $p \rightarrow q$ and $q \rightarrow p$ are true and is false otherwise.

Converse, contrapositive and inverse

$q \to p$

$\sim q \to \sim p$

$\neg p \to \neg q$

- The proposition $q \to p$ is called the **converse** of $p \to q$.
- The **contrapositive** of $p \to q$ is the proposition $\neg q \to \neg p$.
- The proposition $\neg p \to \neg q$ is called the **inverse** of $p \to q$.

- **CONTRAPOSITIVE will have same truth values as $p \to q$**

converse
contra+ve
inverse

Precedence of Logical Operators

- This means that $\neg p \land q$ is the conjunction of $\neg p$ and q, namely,$(\neg p) \land q$, not the negation of the conjunction of p and q, namely $\neg(p \land q)$
- Another general rule of precedence is that the conjunction operator takes precedence over the disjunction operator, so that $p \land q \lor r$ means $(p \land q) \lor r$ rather than $p \land (q \lor r)$.

Operator	*Precedence*
$\neg$	1
$\land$	2
$\lor$	3
$\rightarrow$	4
$\leftrightarrow$	5

Translating English sentence

1. You can access from Internet from campus only if you are computer science or you are not freshman
2. You cannot ride the roller coaster if you are under 4 feets tall unless you are older than 16 years old
3. The automated reply cannot be seen when file system is full

"if p, then q"	"p implies q"
"if p, q"	"p only if 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"
"a necessary condition for p is q"	"q follows from p"
"q unless $\neg p$"	

- PROPOSITONAL EQUIVALENCE

Compound propositions

Compound proposition refer to expression formed from propositional variables using logical operators such as p^q

- **Tautology**: compound proposition that is always true
- **Contradiction/ absurity**: compound proposition that is always false
- **Contingency**: neither tautology neither contradiction.

Tautology and Contradiction example

p	¬p	p ∨ ¬p	p ∧ ¬p
T	F		
F	T		

Tautology and Contradiction example

p	¬p	p ∨ ¬p	p ∧ ¬p
T	F	T	
F	T	T	

Tautology and Contradiction example

p	¬p	p ∨ ¬p	p ∧ ¬p
T	F	T	F
F	T	T	F

Logical Equivalence

if $p \leftrightarrow q$ Tautology

- Definition:
  - We do not say p and q are equal. We say they are logically equivalent or equivalent if $p \leftrightarrow q$ is tautology
- Representation
  - We denote p is equivalent to q by $p \equiv q$ or $p \Leftrightarrow q$
- Establishment of equivalence
  - Construct truth tables
  - Using equivalence laws

$p \equiv q$ or $p \Leftrightarrow q$

Examples

- Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent
- Show that $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent

Equivalent Statements

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

Logical equivalence

IDENTITY LAW BHANEKO J HO TEI AAUNA PARYO
DOMINATION LAW BHANEKO T RA F LE DOMINATE GARNA PARYO

law with implication $p \to q \equiv \neg p \lor q$

Equivalence	*Name*
$p \land \mathbf{T} \equiv p$ $p \lor \mathbf{F} \equiv p$	Identity laws
$p \lor \mathbf{T} \equiv \mathbf{T}$ $p \land \mathbf{F} \equiv \mathbf{F}$	Domination laws
$p \lor p \equiv p$ $p \land p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \lor q \equiv q \lor p$ $p \land q \equiv q \land p$	Commutative laws
$(p \lor q) \lor r \equiv p \lor (q \lor r)$ $(p \land q) \land r \equiv p \land (q \land r)$	Associative laws
$p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$ $p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$	Distributive laws
$\neg(p \land q) \equiv \neg p \lor \neg q$ $\neg(p \lor q) \equiv \neg p \land \neg q$	De Morgan's laws

Examples

- Show that $\neg(p \to q)$ and $p \land \neg q$ are logically equivalent
  - Law of implication
  - De Morgan Law
  - Double negation law

- Show that $(p \to q) \land (p \to r) \equiv p \to (q \land r)$: by equivalence laws
  - Law with implication on both sides
  - Distribution law on LHS

PREDICATE LOGIC AND QUANTIFIERS

- Last section: proposition, compound proposition. Now predicate
- The statement “x is greater than 3” has two parts
  - First part, variable x, is subject of statement
  - Second part, predicate,” is greater than 3” is property of subject
- We can denote statement “ x is greater than 3” is denoted by P(x), where P denotes predicate and x is variable
- The statement P(x)– propositional function P at x
- Once value has been assigned to variable x, the statement P(x) becomes proposition and has truth value

PREDICATE LOGIC AND QUANTIFIERS

- Universal Quantification
  - The universal quantification of a predicate P(x) is statement " For all values of x, P(x) is true"
  - Denoted by $\forall x$ P(x)
  - Read as
    - for all x P(x)
    - for every x P(x)
  - An element for which P(x) is false is called counterexample of $\forall x$ P(x)

  - When all the elements in the domain can be listed—say, x_1, x_2,..., x_n—it follows that the universal quantification $\forall x P(x)$ is the same as the conjunction

$$P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n),$$

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

Universal Existential

PREDICATE LOGIC AND QUANTIFIERS

- Universal Quantification
- Example:
  - Let P(x) be statement "x+1>x" what is truth value of $\forall x$ P(x)
  - Let Q(x) be statement "x<2". What is truth value of $\forall x$ P(x)

PREDICATE LOGIC AND QUANTIFIERS

- **Existential Quantification**
  - The existential quantification of a predicate P(x) is statement " There exists a value of x for which P(x) is true"
  - Denoted by $\exists x$ P(x)
  - Read as
    - There is an x such that P(x)
    - There is at least one x such that P(x)

  - When all elements in the domain can be listed—say, $x_1, x_2, \ldots, x_n$— the existential quantification $\exists x P(x)$ is the same as the disjunction

    $P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n)$,

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

PREDICATE LOGIC AND QUANTIFIERS

- Existential Quantification
- Example
  - Let P(x) denote statement "x=x+1". What is truth value of $\exists x$ P(x)
  - What is the truth value of $\exists x P(x)$, where P (x) is the statement "$x^2 > 10$" and the universe of discourse consists of the positive integers not exceeding 4?

PREDICATE LOGIC AND QUANTIFIERS

- $\forall$ and $\exists$ have higher precedence than all logical operators from propositional calculus

TABLE 1 **Quantifiers.**		
Statement	***When True?***	***When False?***
$\forall x P(x)$	$P(x)$ is true for every x.	There is an x for which $P(x)$ is false.
$\exists x P(x)$	There is an x for which $P(x)$ is true.	$P(x)$ is false for every x.

Disproof by Counterexample

- A counterexample to $\forall x\, P(x)$ is an object c so that $P(c)$ is false.

- Statements such as $\forall x\, (P(x) \rightarrow Q(x))$ can be disproved by simply providing a counterexample.

Statement: “All birds can fly.”

Disproved by counterexample: Penguin.

Negation

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

- $\neg(\forall x\ P(x))$ is logically equivalent to $\exists x\ (\neg P(x))$.

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

- $\neg(\exists x\ P(x))$ is logically equivalent to $\forall x\ (\neg P(x))$.

- **This is de Morgan's law for quantifiers**

Negation	*Equivalent Statement*	*When Is Negation True?*	*When False?*
$\neg\exists x P(x)$	$\forall x \neg P(x)$	For every x, $P(x)$ is false.	There is an x for which $P(x)$ is true.
$\neg\forall x P(x)$	$\exists x \neg P(x)$	There is an x for which $P(x)$ is false.	$P(x)$ is true for every x.

Proof given in book. Read yourself

Nested quantifier

- where one quantifier is within the scope of another, such as
  $\forall x \exists y\ (x + y = 0)$

for every x there exits a y such that p x

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

Examples

- Use P(x): x is even;
- Q(x): x is prime number, and
- R(x,y):x+y is even. variables x and y represent integers

1. Write an English sentence corresponding to
   $a)$ $\forall x$ P(x) (b) $\exists$x Q(x)
2. Write an English sentence corresponding to
   (a) $\forall x\exists$y R(x,y) (b) $\exists$x $\forall y$ R(x,y)
3. Write an English sentence corresponding to
   (a) $\forall x$($\neg$(Q(x)) (b) $\exists$y ($\neg$P(y)
4. Write an English sentence corresponding to
   $(a)$$\neg$ ($\exists$x P(x)) (b) $\neg$($\forall x$ Q(x))
5. Determine truth statement to each of above

1. a) For all x, P(x) is even
b) there exists x such that Q(x) is odd
2 a) For all x, there exists y such that x+y is even
b) there exist x such that for all y x+y is even
3 a) For all x, x is not prime number
b) there exist y such that y is not even
4 a) It is not true that there exist x such that x is even
b) it is not true that for all x such that every number is prime number
5. (F, T) (T, F) (F,T), (F,T)

Examples

45

- Translate the statement

$\forall x(C(x) \vee \exists y(C(y) \wedge F(x, y)))$

into English, where $C(x)$ is “x has a computer,” $F(x, y)$ is “x and y are friends,” and the domain for both x and y consists of all students in your school.

- Express the statement “If a person is female and is a parent, then this person is someone’s mother” as a logical expression involving predicates, quantifiers with a domain consisting of all people, and logical connectives

  - **every student in your school has a computer or has a friend who has a computer**
  - **$\forall x((F(x) \wedge P(x)) \rightarrow \exists y M(x, y))$.**

Rule of Inference

Definition:

$$\begin{array}{l} P_1 \\ \underline{P_2} \\ Q \end{array}$$

is a inference rule if $(P_1 \wedge P_2) \rightarrow Q$ is a tautology.

Rules of Inference

- The general form of a rule of inference is:

- p_1
- p_2
- .
- .
- .
- p_n
- _____
- $\therefore\ q$

The rule states that if p_1 and p_2 and … and p_n are all true, then q is true as well.

Each rule is an established tautology of

$$p_1 \land p_2 \land \ldots \land p_n \land q$$

These rules of inference can be used in any mathematical argument and do not require any proof.

Definition

- **Argument**: sequence of propositions
- **Premises/Hypothesis**: except final proposition
- **Conclusion**: final proposition

An argument is valid if truth of all premises implies that conclusion is true

Rules of Inference provide the templates or guidelines for constructing valid arguments from the statements that we already have.

Rules of Inference

- **Rules of inference** provide the justification of the steps used in a proof.

- One important rule is called **modus ponens** or the **law of detachment**. It is based on the tautology $(p \wedge (p \to q)) \to q$. We write it in the following way:

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

The two hypotheses p and $p \to q$ are written in a column, and the conclusion below a bar, where $\therefore$ means "therefore".

- Write truth table of $\mathbf{p}$, $\mathbf{q}$, $\mathbf{p} \rightarrow \mathbf{q}$, $\mathbf{p} \wedge (\mathbf{p} \rightarrow \mathbf{q})$, $\mathbf{p} \wedge (\mathbf{p} \rightarrow \mathbf{q}) \rightarrow \mathbf{q}$,

Examples

- “ If you have access to network, you can change your grade”
- You have access to network

∴You can change your grade

DIFFERENT RULES

CONJUNCTION

P

Q

$\therefore P \wedge Q$

SIMPLIFICATION

$P \wedge Q$

$\therefore P$

MODUS TOLLENS

$P \rightarrow Q$

$\neg Q$

$\therefore \neg P$

DISJUNCTIVE SYLLOGISM

$\neg P$

$P \vee Q$

$\therefore Q$

MODUS PONENS

$P \rightarrow Q$

P

$\therefore Q$

HYPOTHETICAL SYLLOGISM

$P \rightarrow Q$

$Q \rightarrow R$

$\therefore P \rightarrow R$

ADDITION

P

$\therefore P \vee Q$

Example

Is the following argument valid?

If taxes are lowered, then income rises.

Income rises.

$\therefore$ Taxes are lowered.

"If $\sqrt{2} > \frac{3}{2}$, then $(\sqrt{2})^2 > \left(\frac{3}{2}\right)^2$. We know that $\sqrt{2} > \frac{3}{2}$. Consequently, $(\sqrt{2})^2 = 2 > \left(\frac{3}{2}\right)^2 = \frac{9}{4}$."

Example

- State which rule of inference is the basis of the following argument: “It is below freezing now. Therefore, it is either below freezing or raining now.”
- **addition rule**
- State which rule of inference is the basis of the following argument: “It is below freezing and raining now. Therefore, it is below freezing now.”
- **simplification rule**

Example

- Show [¬Q ∧ (P → Q)] → ¬P ≡ T

- First, we note $Q \wedge \neg R \equiv \neg(\neg Q \vee R) \equiv \neg(Q \rightarrow R)$.
- So we have the following inference:

(1)	$P \rightarrow (Q \rightarrow R)$	Premise
(2)	$Q \wedge \neg R$	Premise
(3)	$\neg(Q \rightarrow R)$	Logically equivalent to (2)
(4)	$\neg P$	Applying the second implication rule (Modus Tonens) to (1) and (3)

Example

Premises:

P q $\wedge$

a. "It's not sunny and it's colder than yesterday" $\neg p \wedge q$

b. "We will go swimming only if it's sunny." $r \rightarrow p$

c. "If we don't go swimming then we will take canoe trip." $\neg r \rightarrow s$

d. "If we take a canoe trip, then we will be home by sunset." $s \rightarrow t$

Conclusion: "We will be home by sunset." t.

(1)	$\neg p \wedge q$	Premise
(2)	$\neg p$	Simplification rule using (1)
(3)	$r \rightarrow p$	Premise
(4)	$\neg r$	MT using (2) (3)
(5)	$\neg r \rightarrow s$	Premise
(6)	s	MP using (4) (5)
(7)	$s \rightarrow t$	Premise
(8)	t	MP using (6) (7)

Example

p

- 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."

t

Step	Reason
1. $\neg p \wedge q$	Premise
2. $\neg p$	Simplification using (1)
3. $r \rightarrow p$	Premise
4. $\neg r$	Modus tollens using (2) and (3)
5. $\neg r \rightarrow s$	Premise
6. s	Modus ponens using (4) and (5)
7. $s \rightarrow t$	Premise
8. t	Modus ponens using (6) and (7)

Example

- 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."

Step	**Reason**
1. $p \to q$	Premise
2. $\neg q \to \neg p$	Contrapositive of (1)
3. $\neg p \to r$	Premise
4. $\neg q \to r$	Hypothetical syllogism using (2) and (3)
5. $r \to s$	Premise
6. $\neg q \to s$	Hypothetical syllogism using (4) and (5)

Rules of Inference for Quantified Statements

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

Example

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

1. $\forall x(D(x) \rightarrow C(x))$ Premise
2. $D(\text{Marla}) \rightarrow C(\text{Marla})$ Universal instantiation from (1)
3. $D(\text{Marla})$ Premise
4. $C(\text{Marla})$ Modus ponens from (2) and (3)

Questions

- Show that following argument is valid. If today is Tuesday, I have a test in Mathematics of Economics. If my Economics Professor is sick, I will not have a test in Economics. Today is Tuesday and my Economics Professor is sick. Therefore I have a test in Mathematics.
- 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.”

Methods of Proof/Proving Theorems

- Direct Method
- Indirect method
  - Proof by contradiction
  - Proof by contraposition

Direct Proof

- Direct proof lead from hypothesis of theorem to conclusion.
- It begins with premises, continue with sequence of deductions, and end with conclusion
- An implication $p \to q$ can be proved by showing that if p is true, then q is also true.

Direct Proof

1. If n is an odd integer, then n^2 is odd.
2. If m and n are both perfect squares, then nm is also perfect square

Indirect Proof

- Contrapositive
  - An implication $p \to q$ is equivalent to its **contra-positive** $\neg q \to \neg p$. Therefore, we can prove $p \to q$ by showing that whenever q is false, then p is also false.
- Examples

1. Prove that if n is an integer, and 3n+2 is odd, then n is odd
2. Let n be an integer. Prove that if n^2 is odd, then n is odd.
3. Prove that if n=ab, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

Indirect Proof

- Contradiction
  - To prove a statement P is true, we begin by assuming P is false and shows that this leads to contradiction. Something that always false.
- Example

1. Show that $\sqrt{2}$ is irrational by proof of contradiction
   1. $\sqrt{2}$= a/b (assume it is rational)
   2. $2=a^2/b^2$;$a^2=2b^2$; thus a is even; so a=2k
   3. $4k^2=2b^2$; $b^2=2k^2$;
   4. Which proves b is even.
   5. So both a and b have 2 in common. So $\sqrt{2}$ is not rational

Indirect Proof

- Contradiction
  - Many statements are in form P→Q, which when negated has form P→ $\neg Q$. This means for sake of contradiction P is true but Q is false. When this result is not true, then it must be that Q is true.
- Example

1. Give a proof by contradiction of the theorem "If 3n + 2 is odd, then n is odd."
   1. p="3n+2 is odd" and q="n is odd"
   2. Assume both p and ¬q are true
   3. q:n=2k; p=3(2k)+2.=2(3k+1)
   4. It seems that p is even. But our assumption is that p is odd
   5. Now since there is contradiction, p→q is true

Example

Use a direct proof, a contrapositive proof, or a proof by contradiction to prove each of the following propositions.

Proposition

Suppose $a, b \in \mathbb{Z}$. *If* $a + b \geq 19$, *then* $a \geq 10$ *or* $b \geq 10$.

Proposition

Suppose $a, b, c, d \in \mathbb{Z}$ *and* $n \in \mathbb{N}$. *If* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $a + c \equiv b + d \pmod{n}$.

Proposition

Suppose n *is a composite integer. Then* n *has a prime divisor less than or equal to* $\sqrt{n}$.

Question 1

- For any integers a and b, if a+b>=19, then a>=10 or b>= 10
- Solution: contrapositive
  - If its not case a>=10 or b >=10, then its not case a+b>=19
  - If (not a>=10) and (not b>=10) then not a+b>=19

    [Demorgan's law: $\overline{\mathrm{A} \cup \mathrm{B}}=\bar{A} \cap \bar{B}$]
  - If (a<10) and (b<10) then a+b<19
  - If (a<=9) and (b<=9) then a+b<19
  - Adding these two together, a+b<19 (9+9=18)

Question 2

- If $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$, then $a+c \equiv (b+d) \pmod{n}$
- Solution: Direct method
  - $(a-b) = kn$; $(c-d) = ln$;
  - $(a-b)+(c-d) = kn+ln$;
  - $(a+c)-(b+d) = (k+l)n$
- If $a \equiv b \pmod{n}$, then $a^2 \equiv b^2 \pmod{n}$.
  - If $a-b=kn$;
  - $(a-b)(a+b)=kn(a+b)$
  - $a^2-b^2=k(a+b)n$

Question 3

- Contradiction method:
- By definition of composite integer, n=ab
- There is a factor with 1<a<n. and 1<b<n (composite)
- a$\leq b$
- **Suppose contradiction is true**
- If a>$\sqrt{n} and\ b > \sqrt{n}, then\ ab > n$ which is contradiction
- So a $\leq \sqrt{n}\ or\ b \leq \sqrt{n}.$
- Thus n has positive divisor not exceeding $\sqrt{n}$

Induction

- The **principle of mathematical induction** is a useful tool for proving that a certain predicate is true for **all natural numbers**.

- It cannot be used to discover theorems, but only to prove them.

Induction

- If we have a propositional function P(n), and we want to prove that P(n) is true for any natural number n, we do the following:

- Show that P(0) is true.
  (basis step)
- Show that if P(n) then P(n + 1) for any $n \in N$.
  (inductive step)
- Then P(n) must be true for any $n \in N$.
  (**conclusion**)

Induction

- **Example one**

- Show that $n < 2^n$ for all positive integers n.

- Let P(n) be the proposition “$n < 2^n$.”

- 1. Show that P(1) is true.
  (basis step)

- P(1) is true, because $1 < 2^1 = 2$.

Induction

2. Show that if P(n) is true, then P(n + 1) is true.
(inductive step)

- Assume that $n < 2^n$ is true.
- We need to show that P(n + 1) is true, i.e.
- $n + 1 < 2^{n+1}$

- We start from $n < 2^n$;
- Add 1 to both sides
- $n + 1 < 2^n + 1 \le 2^n + 2^n = 2^{n+1}$
- Therefore, if $n < 2^n$ then $n + 1 < 2^{n+1}$

Induction

Then P(n) must be true for any positive integer. (conclusion)

- $n < 2^n$ is true for any positive integer.
- End of proof.

Induction

Example Two ("Gauss"):

- $1 + 2 + \ldots + n = n(n + 1)/2$

- Show that P(0) is true.
  (basis step)

- For n = 0 we get 0 = 0. True.

Induction

Show that if P(n) then P(n + 1) for any $n \in N$. (inductive step)

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

Induction

Then P(n) must be true for any $n \in N$. (conclusion)

- $1 + 2 + \ldots + n = n (n + 1)/2$ is true for all $n \in N$.
- End of proof.

Example 3: Let $A_1, A_2, A_3, \ldots, A_n$ be any n sets. We show by mathematical induction that

$$\overline{\left(\bigcup_{i=1}^{n} A_i\right)} = \bigcap_{i=1}^{n} \overline{A_i}\,.$$

Solutions

Basis Step. P(1) is the statement $\overline{A_1} = \overline{A_1}$, which is obviously true.

Induction Step. If P(k) is true for any k sets, then the left-hand side of

P($k+1$) is $\overline{\left(\bigcup_{i=1}^{k+1} A_i\right)} = \overline{A_1 \cup A_2 \cup \cdots \cup A_k \cup A_{k+1}}$

$= \overline{(A_1 \cup A_2 \cup \cdots \cup A_k) \cup A_{k+1}}$ Associative property of $\cup$

$= \overline{(A_1 \cup A_2 \cup \cdots \cup A_k)} \cap \overline{A_{k+1}}$ By De Morgan's law for two sets

$= \left(\bigcap_{i=1} \overline{A_i}\right) \cap \overline{A_{k+1}}$ Using P(k)

$= \bigcap_{i=1}^{k+1} \overline{A_i}.$

- **Example four**: $n!=n*(n-1)!$
- Basic step: $1!=1$
- Induction step:
- For n is true
- $n!=n*(n-1)!$
- Multiplying by $(n+1)$,
- $n!*(n+1)=n*(n-1)!*(n+1)$
- $(n+1)!=n!*(n+1)=(n+1)*((n+1)-1)!$

Solve using induction

FUNCTION SQ(A)

1. $C \leftarrow 0$
2. $D \leftarrow 0$
3. **WHILE** ($D \neq A$)
    a. $C \leftarrow C + A$
    b. $D \leftarrow D + 1$
4. **RETURN** (C)

END OF FUNCTION SQ

FUNCTION GCD(X, Y)

1. **WHILE** ($X \neq Y$)
    a. **IF** ($X > Y$) **THEN**
        1. $X \leftarrow X - Y$
    b. **ELSE**
        1. $Y \leftarrow Y - X$
2. **RETURN** (X)

END OF FUNCTION GCD

Basis Step. P(0) is the statement $C_0 = A \times D_0$, which is true since the value of both C and D is zero "after" zero passes through the **WHILE** loop.

Induction Step. We must now use

$$P(k): C_k = A \times D_k \tag{2}$$

to show that $P(k+1): C_{k+1} = A \times D_{k+1}$. After a pass through the loop, C is increased by A, and D is increased by 1, so $C_{k+1} = C_k + A$ and $D_{k+1} = D_k + 1$.

$$\begin{aligned}
\text{left-hand side of } P(k+1): \quad C_{k+1} &= C_k + A \\
&= A \times D_k + A && \text{Using (2) to replace } C_k \\
&= A \times (D_k + 1) && \text{Factoring} \\
&= A \times D_{k+1}. && \text{Right-hand side of } P(k+1)
\end{aligned}$$

By the principle of mathematical induction, it follows that as long as looping occurs $C_n = A \times D_n$. The loop must terminate. (Why?) When the loop terminates, $D = A$, so $C = A \times A$, or A^2, and this is the value returned by the function SQ. ◆

Theorem 5. *If a and b are in Z^+, then* $\mathrm{GCD}(a, b) = \mathrm{GCD}(b, b \pm a)$.

Proof: If c divides a and b, it divides $b \pm a$, by Theorem 2. Since $a = b - (b - a) = -b + (b + a)$, we see, also by Theorem 2, that a common divisor of b and $b \pm a$ also divides a and b. Since a and b have the same common divisors as b and $b \pm a$, they must have the same greatest common divisor. ◆

We claim that if X and Y are positive integers, then GCD returns $\mathrm{GCD}(X, Y)$. To prove this, let X_n and Y_n be the values of X and Y after $n \geq 0$ passes through the **WHILE** loop. We claim that $P(n)$: $\mathrm{GCD}(X_n, Y_n) = \mathrm{GCD}(X, Y)$ is true for all $n \geq 0$, and we prove this by mathematical induction. Here n_0 is 0.

Basis Step. $X_0 = X$, $Y_0 = Y$, since these are the values of the variables before looping begins; thus $P(0)$ is the statement $\mathrm{GCD}(X_0, Y_0) = \mathrm{GCD}(X, Y)$, which is true.

Induction Step. Now let us consider the left-hand side of $P(k + 1)$, that is, $\mathrm{GCD}(X_{k+1}, Y_{k+1})$. After the $k + 1$ pass through the loop, either $X_{k+1} = X_k$ and $Y_{k+1} = Y_k - X_k$ or $X_{k+1} = X_k - Y_k$ and $Y_{k+1} = Y_k$. Then, if $P(k)$: $\mathrm{GCD}(X_k, Y_k) = \mathrm{GCD}(X, Y)$ is true, we have by Theorem 5, Section 1.4, that $\mathrm{GCD}(X_{k+1}, Y_{k+1}) = \mathrm{GCD}(X_k, Y_k) = \mathrm{GCD}(X, Y)$. Thus, by the principle of mathematical induction, $P(n)$ is true for all $n \geq 0$. The exit condition for the loop is $X_n = Y_n$, and we have $\mathrm{GCD}(X_n, Y_n) = X_n$. Hence the function always returns the value $\mathrm{GCD}(X, Y)$. ◆