# [Mathematical Reasoning]

Discrete Structures (CSc 511)

**Samujjwal Bhandari**

Central Department of Computer Science and Information Technology (CDCSIT)

Tribhuvan University, Kirtipur,

Kathmandu, Nepal.

# Mathematical Reasoning

Any of the mathematical statement must be supported by arguments that make it correct. For this we need to know different techniques and rules that can be applied in the mathematical statements such that we can prove the correctness of the given mathematical statement. This method of understanding the correctness by sequence of statements forming an argument is a proof of the statement. A theorem is a mathematical statement that can be shown to be true. Well founded proof is the steps of mathematical statements that present an argument that makes the theorem true. By proving some mathematical problem we mean that we solve that problem. For this purpose valid steps are required such that as mentioned above those steps aid on solving the problems. Problem solving or proving is not just a science so there is no hard and fast rule that is applied in problem solving. However there are some guiding methods that help us to solve different kinds of problems. Here still we must note that the problem solving is not just a science, so hard work and art is needed.

# Rules of Inference

To draw conclusion from the given premise we must be able to apply some well defined steps that helps reaching the conclusion. These steps of reaching the conclusion are provided by the rules of inference. Here some of the rules of inferences are given below:

**Rule 1: Modus Ponens (or Law of Detachment)**

Whenever two propositions p and p → q are both true then we confirm that q is true. We write this rule as

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

, This rule is valid rule of inference because the implication $[p \wedge (p \to q)] \to q$ is a tautology.

**Example:**

Ram is hard working and if Ram is hard working, then he is intelligent. By modus ponens (verify!!!), this logically infers Ram is intelligent.

**Rule 2: Hypothetical Syllogism (Transitive Rule)**

Whenever two propositions p→ q and q → r are both true then we confirm that implication p → q is true. We write this rule as

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

, This rule is valid rule of inference because the implication [(p→ q) ∧ (q→ r)] → (p→ r) is a tautology.

This rule can be extended to larger numbers of implications as

$$\begin{array}{l} p \to q \\ q \to r \\ \underline{r \to s} \\ \therefore p \to s \end{array}$$

**Example:**

If today is Sunday, then today is rainy day and if today is rainy day, then it is wet today. By transitivity rule (verify!!!), this logically infers It is wet today.

In similar fashion we can define the following rules.

**Rule 3: Addition**

Due to the tautology p→ (p ∨ q), rule $\dfrac{p}{\therefore p \vee q}$ is a valid rule of inference.

**Rule 4: Simplification**

Due to the tautology (p ∧ q) → p, rule $\dfrac{p \wedge q}{\therefore p}$ is a valid rule of inference.

**Rule 5: Conjunction**

Due to the tautology [(p) ∧ (q)]→ (p ∧ q), rule $\begin{array}{c} p \\ \underline{q} \\ \therefore p \wedge q \end{array}$ is a valid rule of inference.

**Rule 6: Modes Tollens**

Due to the tautology [¬q ∧ (p→ q)] → ¬p, rule $\begin{array}{l} \neg q \\ p \to q \\ \hline \therefore \neg p \end{array}$ is a valid rule of inference.

**Rule 7: Disjunctive Syllogism**

Due to the tautology [(p ∨ q) ∧ ¬p]→ q, rule $\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$ is a valid rule of inference.

**Rule 8: Constructive Dilemma**

Due to the tautology [(p→ q) ∧ (r→ s) ∧ (p ∨ r)] → (q ∨ s), rule $\begin{array}{l} (p \to q) \wedge (r \to s) \\ p \vee r \\ \hline \therefore q \vee s \end{array}$ is a valid rule of inference.

**Rule 9: Destructive Dilemma**

Due to the tautology [(p→ q) ∧ (r→ s) ∧ (¬q ∨ ¬s)] → (¬p ∨ ¬r), rule $\begin{array}{l} (p \to q) \wedge (r \to s) \\ \neg p \vee \neg s \\ \hline \therefore \neg p \vee \neg r \end{array}$ is a valid rule of inference.

**Rule 10: Resolution**

Due to the tautology [(p ∨ q) ∧ (¬p ∨ r)]→ (q ∨ r), rule $\begin{array}{l} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$ is a valid rule of inference.

## Valid Arguments

An argument is called valid if all hypotheses are true and the conclusion is also true. We can conclude that the implication $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \to q$ is tautology. If all the propositions in the valid argument are true then the conclusion is true.

Sometime valid argument can lead to incorrect conclusion if one or more of the false premises are used in the argument. For e.g. If CDCSIT is at Kirtipur, then Lagankhel is at Kirtipur. CDCSIT is at Kirtipur. Consequently, Lagankhel is at Kirtipur.

The above argument is a valid argument using the rule modus ponens. However the conclusion of the argument is false since the proposition at the hypothesis “Lagankhel is at Kirtipur” is false that means conclusion may be false here.

**Example 1:** Construct an argument using rules of inference to show that the hypotheses “If it does not rain or if it is not foggy, then the sailing race will be held and the life saving demonstration will go on,” “ If the sailing race is held, then the trophy will be awarded,’ and “The trophy was not awarded” imply the conclusion “ It rained”.

**Solution:**

Let p = “It rains”, q = “It is foggy”, r = “the sailing race is held”, s = “Life saving demonstration is done”, and t = “ Trophy is awarded”.

Then we have to show that the argument

$[((\neg p \vee \neg q) \rightarrow (r \wedge s)) \wedge (r \rightarrow t) \wedge \neg t] \rightarrow p$ is valid.

[1] $(r \rightarrow t)$ [Hypothesis]

[2] $\neg t$ [Hypothesis]

[3] $\neg r$ [Modus Tollens using steps 1 and 2]

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

[5] $\neg(\neg p \vee \neg q) \vee (r \wedge s)$ [Implication of Step 4]

[6] $(p \wedge q) \vee (r \wedge s)$ [De Morgan’s Law in Step 5]

[7] $p \vee (r \wedge s)$ [Simplification using step 6]

[8] $p \vee r$ [Simplification using step 7]

Here our original premises changes to $(p \vee r) \wedge \neg r$ [from step 8 and 3]

[9] $r \vee p$ [Commutative law in step 8]

[10] $\neg r \vee p$ [Addition using step 3]

[11] $p \vee p$ [Resolution using steps 9 and 10]

[12] $p$ [Idempotent law]

Hence argument is valid. With conclusion “It rained”.

**Example 2:** For the set of premises "If I play hockey, then I am sore the next day." "I use the whirlpool if I am sore." " I did not use the whirlpool". What relevant conclusion can be drawn? Explain the rules of inference used to draw the conclusion.

**Solution:**

Let p = "I play hockey", q = " I am sore", r = "I use the whirlpool"

Then the above premises are

a) $p\rightarrow q$

b) $q\rightarrow r$

c) $\neg r$

Using hypothetical syllogism in premises a and b we have $p\rightarrow r$ i.e. "if I play hockey, then I use whirlpool"

Using the modus tollens in premise c and inferred proposition $p\rightarrow r$ we conclude $\neg p$ is true i.e. p is false. p is false means " I did not play hockey".

# Fallacies

The fallacies are arguments that are convincing but not correct. So fallacies produce faulty inferences. So fallacies are contingencies rather than tautologies. Here we talk different fallacies that we may encounter.

**Fallacy of affirming the conclusion (consequence)**

This kind of fallacy has the form $\begin{array}{c} q \\ p \rightarrow q \\ \hline \therefore p \end{array}$ i.e. $p \wedge (p\rightarrow q) \rightarrow q$. This is not a tautology hence it is a fallacy.

**Example:**

If economy of Nepal is poor, then the education system in Nepal will be poor. The education system in Nepal is poor. Therefore, Economy of Nepal is poor.

In this argument above the conclusion can be false even if both the propositions "If economy of Nepal is poor, then the education system in Nepal will be poor" and "The education system in Nepal is poor" are true. Denoting with symbols we may write $(p\rightarrow q)$

for first proposition and then the second proposition becomes q. this takes the form $q \wedge (p \rightarrow q) \rightarrow q$, which is not a tautology. Since the education system may not depend on the economy of the country.

**Fallacy of denying the hypothesis**

This kind of fallacy has the form $\begin{array}{c} \neg p \\ \underline{p \rightarrow q} \\ \therefore \neg q \end{array}$ i.e. $\neg p \wedge (p \rightarrow q) \rightarrow \neg q$. This is not a tautology hence it is a fallacy.

**Example:**

If today is Sunday, then it rains today. Today is not Sunday. Therefore, it does not rain today. This argument is not true since even if today is not Sunday and it is raining today then the first premise is true and second premise is also true but not the conclusion.

**The non sequitur fallacy**

Non sequitur mean “does not follow”. Generally all logical errors are the cases of non sequitur fallacy. For e.g. $\begin{array}{c} \underline{p} \\ \therefore q \end{array}$, if p is true and q is false then what happens?

**Example:**

I am a teacher therefore Ram is a doctor. (how is this valid? No, it is not i.e. if Ram is not a doctor then what?).

**Begging the Question (Circular Reasoning)**

If the statement that is used for proof is equivalent to the statement that is being proved then it is called circular reasoning.

**Example:**

The square root of 2 is irrational since it is not rational.

Man is mortal because man dies.

Ram is black because he is black.

# Rules of Inference for Quantified Statements

There is a need of other rules to prove assertions that contain open propositions and quantifiers. Some of the rules are:

**Universal Instantiation**

If the proposition of the form ∀xP(x) is supposed to be true then the universal quantifier can be dropped out to get P(c) is true for arbitrary c in the universe of discourse. This can be written as

$$\frac{\forall x P(x)}{\therefore P(c), \text{for all } c}$$

**Example:**

In universe of discourse of all man every man is mortal implies ram is mortal where ram is a man.

**Universal Generalization**

If all the instances of c makes P(c) true, then ∀xP(x) is true. This can be written as

$\frac{P(c), \text{for all } c}{\therefore \forall x P(x)}$, Here the chosen c must be arbitrary, not a specific element from the universe of discourse. This rule is seldom explicitly used.

**Existential Instantiation**

If the proposition of the form ∃xP(x) is supposed to be true then the there is an element c in the universe of discourse such that P(c) is true. This can be written as

$\frac{\exists x P(x)}{\therefore P(c), \text{for some } c}$, Here the element c is not arbitrary, it must be specific such that P(x) is true. We generally find difficulty in finding such c.

**Existential Generalization**

If at least a element c from the universe of discourse makes P(c) true, then ∃xP(x) is true. This can be written as $\frac{P(c), \text{for some } c}{\therefore \exists x P(x)}$

**Inference with quantified statements**

**Example 1:**

Explain which rules of inference are used for the argument "Linda, a student in the class, owns a red convertible. Everyone who owns a red convertible has gotten at least one speeding ticket. Therefore, someone in this class has gotten a speeding ticket."

**Solution:**

Let S(x) denotes x is a student in a class, R(x) denotes x owns red convertible and T(x,y) denotes x has gotten y numbers of speeding tickets. Where x is a set of people, Then

$S(Linda)$ , $R(Linda)$, $\forall x(R(x) \rightarrow \exists yT(x,y))$ are the premises and $\exists x(S(x) \wedge T(x,1))$ is the conclusion.

$R(Linda) \rightarrow \exists yT(Linda,y)$ is true using universal instantiation. Since R(Linda) is true using modes ponens $\exists yT(Linda,y)$ is true. The number 1 is the least number of tickets that can be there. So using existential instantiation T(Linda,1). Since both S(Linda) and T(Linda,1) are true by using conjunction $S(Linda) \wedge T(Linda,1)$. Hence By using existential generalization $\exists x(S(x) \wedge T(x,1))$ is true.

**Example 2:**

Prove or disprove the validity of the argument " every living thing is a plant or an animal", "Hari's dog is alive and it is not a plant", "All animals have heart", Hence "Hari's dog has a heart".

**Solution:**

Let P(x) be x is a plant, A(x) be x is an animal, L(x) be x is alive, H(x) be x has heart and d be Hari's dog.

| | | |
|---|---|---|
| [1] | $\forall x(P(x) \vee A(x))$ | [Hypothesis] |
| [2] | $L(d) \wedge \neg P(d)$ | [Hypothesis] |
| [3] | $\forall x(A(x) \rightarrow H(x))$ | [Hypothesis] |
| [4] | $P(d) \vee A(d)$ | [Universal instantiation from 1] |
| [5] | $\neg P(d)$ | [from 2 Simplification] |
| [6] | $A(d)$ | [Disjunctive Syllogism form 4 and 5] |

[7] A(d) → H(d) [Universal instantiation from 3]

[8] H(d) [modus ponens from 6 and 7]

Hence Hari's dog has a heart, so the above argument is valid.

# Proving Theorems

In this part we see Methods of Proof of an Implication. We present different methods here but it is not true that all the methods of proof are given here.

## Direct Proofs

We prove the implication p → q, where we start assuming that the hypothesis i.e. p is true and using information already available (rules of inferences, theorems, etc.), if q becomes true, then the argument becomes valid. This is direct proof.

**Example:**

If a and b are odd integers, then a + b is an even integer.

**Proof:**

We know the fact that if a number is even then we can represent it as 2k, where k is an integer and if the number is odd then it can be written as 2l + 1, where l is an integer. Assume that a = 2k + 1 and b = 2l + 1, for some integers k and m. then a + b = 2k + 1 + 2l + 1 = 2(k + l + 1), here (k + l + 1) is an integer. Hence a + b is even integer.

## Indirect Proofs

We have p → q ≡ ¬q → ¬p i.e. contrapositive of implication is equivalent to the implication. This is the base for indirect proof. We prove the implication p → q by assuming that the conclusion is false and using the known facts we show that the hypothesis is also false.

**Example:**

If the product of two integers a and b is even, then either a is even or b is even.

**Proof:**

Suppose both a and b are odd, then we have a = 2k + 1 and b = 2l + 1.

So $ab = (2k + 1)(2l + 1) = 4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1$, i.e. ab is an odd number. Hence both a and b being odd implies ab is also odd. This is indirect proof.

## Trivial and Vacuous Proofs

If it is possible to show that q is correct regardless of truth value of p then we can say that implication $p \to q$ is true. This is **trivial proof**. If we can show that p is false then the implication $p \to q$ is true. This is **vacuous proof**.

**Example:**

If x is an integer, then 3 is an odd integer. (Trivial)

If a black is white, then pink is blue. (Vacuous)

## Proofs by Contradiction

The steps in proof of implication $p \to q$ by contradiction are:

Assume $p \wedge \neg q$ is true.

Try to so that the above assumption is false

When the assumption is found to be false then implication $p \to q$ is true since $p \to q$ is equivalent to $\neg p \vee q$ and negation of $\neg p \vee q$ is $p \wedge \neg q$ (By De Morgan's Law), so if our assumption is false then its negation is true.

Alternately,

Contradict the statement and show that this leads to the false conclusion; if this is true then the contradicted statement must be false (since $\neg p \to \mathbf{F}$ is true only if $\neg p$ is false), hence the statement is true.

**Example:**

If $a^2$ is an even number, then a is an even number.

**Proof:**

Assume that $a^2$ is an even number and a is an odd number. Since a is an odd number we have $a = 2k + 1$, for some integer k. so $a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(k^2 + k) + 1$, here $k^2 + k$ is some integer, say l, then $a^2 = 2l + 1$ i.e. $a^2$ is an odd number This contradicts our assumption that is $a^2$ even. Hence the proof.

## Proof by Cases

The implication of the form $(p_1 \lor p_2 \lor \dots \lor p_n) \to q$ can be prove by using the tautology $(p_1 \lor p_2 \lor \dots \lor p_n) \to q \leftrightarrow [(p_1 \to q) \land (p_2 \to q) \land \dots \land (p_n \to q)]$, i.e. we can show every implication $(p_i \to q)$ true for i =1, 2, …, n.

**Example:**

If $|x| > 3$, then $x^2 > 9$, where x is a real number.

**Proof:**

Here we have to consider two cases $-x > 3$ and $x > 3$ since $|x|$, is an absolute value of x, is x when $x \geq 0$ and $-x$ when $x \leq 0$. If $-x > 3$, then $x^2 > 9$. Similarly, if $x > 3$, then $x^2 > 9$.

## Proof of Equivalence

We can prove the equivalence i.e. $p \leftrightarrow q$ by showing $p \to q$ and $q \to p$ both.

**Example:**

Prove that if n is a positive integer, then n is even if and only if 7n + 4 is even.

**Proof:**

Assume n is even then we have an integer k such that n = 2k, so 7n + 4 = 7*2k +4 = 2(7k +2) here 7k + 4 is an integer so that 7n + 4 = 2l, where l =7k + 2 i.e. 7n + 4 is even. By direct proof it is proved that if n is even, then 7n + 4 is even.

Assume n is odd then we have an integer m such that n = 2m + 1, then 7n + 4 = 14m +7 + 4 = 2(7m + 5) +1here since 7m + 5 is an integer 7n + 4 is an odd number by indirect proof it is proved that if 7n + 4 is even, then n is even.

Hence the proof.

## Existence Proofs

A proof of a proposition of the form $\exists x P(x)$ is called an existence proof. There are different ways of proving a theorem of this type. Sometime some element a is found to show P(a) to be true, this is called **constructive existence proof**. In other method we do not provide a such that P(a) is true but prove that $\exists x P(x)$ is true in different way, this is called **nonconstructive existence proof**.

**Example: Constructive**

Prove that there are 100 consecutive positive integers that are not perfect squares.

**Proof:**

Lets consider 2500 this is a perfect square of 50, and take 2601 this is a perfect square of 51. in between 2601 and 2500 there are 100 consecutive positive integers. Hence the proof.

**Example: Nonconstructive**

Prove that there is a rational number x and an irrational number y such that $x^y$ is irrational.

**Proof:**

Lets take x = 2 and y = $\sqrt{2}$ then $2^{\sqrt{2}}$ is either rational or irrational. If it is irrational we are done, if it is not irrational then it is rational. So take x = $2^{\sqrt{2}}$ and y = $\sqrt{2}/4$ then we have $(2^{\sqrt{2}})^{\sqrt{2}/4} = 2^{2/4} = \sqrt{2}$ (irrational). Hence there is a rational number x and irrational number y such that $x^y$ is irrational.

## Uniqueness Proofs

To prove the theorem that asserts the existence of unique element with particular property we must show that the element with this property exists and no other elements has this property. There are two parts in this uniqueness proof

Existence: here we show that the element with desire property exists

Uniqueness: we show that if $y \neq x$, then y does not have the desired property.

The above two steps can be proved if we prove the statement

$\exists x(P(x) \wedge \forall y(y \neq x \rightarrow \neg P(y)))$.

**Example:**

Show that if a, b, and c are real numbers and $a \neq 0$, then there is a unique solution of the equation $ax + b = c$.

**Proof:**

From the equation $ax + b = c$ we get the solution as $x = (c - b)/a$ (since $a \neq 0$, it is possible). This solution is unique because there is no other value for x than $(c - b)/a$ (a real number).

## Proofs By Counter Examples

To prove that the statement of the form $\forall x P(x)$ is false, we just need some value of x. So while proving for falsity we just look for counter example.

**Example:**

Prove or disprove the product of two irrational numbers is irrational.

Proof:

Here we instantly try to get the product of the irrational to try it. Lets take both the number for product be $\sqrt{2}$ then we have $\sqrt{2}*\sqrt{2} = 2$ (not rational). Hence by counter example it is shown that the product of two irrational numbers is not necessarily irrational.

# Proof Strategies

As mentioned before finding proof is not just a science but an art too, there are no exact rules and strategies for proving the statement. Few strategies that will be very helpful in proving the statement are presented here.

## Forward and Backward Reasoning

Remember the proof strategy utilized by direct proof method. In this method we prove the implication $p \rightarrow q$ starting from p and using known theorems and axioms we come out with q. This type of reasoning is called forward reasoning. Sometimes it is difficult to prove in above way, particularly when the conclusion is complex one. To prove such statements we find p with the help of property that $p \rightarrow q$. this is called backward reasoning or find some property such that q is true, then show that we can come up to the property using p working from the property itself.

**Example: Backward Reasoning**

For integer a, b, c, d and positive integer n, prove that if $a \equiv b \pmod{n}$, and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.

**Proof:**

We can prove $a + c \equiv b + d \pmod{n}$ if we can show that $(a + c) - (b + d) = n.k$ , for some integer k (recall definition of congruence modulo).but $(a + c) - (b + d) = (a - b) + (c - d)$.

We know a – b = n.l, and c –d =n.m, for some integers l and m (see hypothesis). So we can see that (a + c) – (b + d) = n.l + n.m = n(l + m). Here l +m is also an integer, say k, then we have (a + c) – (b + d) = n.k. we have shown that for some integer k, (a + c) – (b + d) = n.k, hence a + c ≡ b + d (modn).

## Using Proof by Cases

When there is no clear way to begin proof but you can sense that the information from different cases moves forward to the proof, you generally use proof by cases (see above on the section proofs by cases for example).

## Techniques from Existing Proofs

It is generally very easy to prove if existing proofs results or ideas from those proofs are applied. You will see a lot of use of this strategy through out the course.

## Using Counter Examples

Given a conjecture if you think it is to be wrong then you can just give the example that defy the statement given.

# Mathematical Induction

In mathematics there are two ways of arriving at result deductive and inductive. In deductive reasoning based upon the assumption that some statements are premises and axioms, we deduce the other statements on the basis of valid inference. In the inductive reasoning through the experiments and observations we come up with the conjecture for a general rule and try to verify truth of the conjecture. One of the important reasoning that considers positive integers is mathematical induction.

## Principle of Mathematical Induction

Let P(n) be a statement that may be true or false for all positive integers n. To prove P(n) is true for all n ≥ 1 we can prove the following steps.

P(1) is true.

For all k ≥ 1, P(k) implies P(k+1).

Generalizing the above proof method instead of 1 take $n_0$ such that the $n_0$ is the basis for induction then we have the steps to be proved are:

**Basis Step:** Show $P(n_0)$ is true.

**Inductive Hypothesis:** Assume P(k) is true for k = n.

**Inductive Step:** Show that the P(k+1) is true on the basis of Inductive Hypothesis.

Expressing in terms of rule of inference, this proof technique can be written as

$[P(n_0) \wedge \forall k(P(k) \rightarrow P(k+1))] \rightarrow \forall nP(n)$.

**Example 1:**

Prove that $2 - 2.7 + 2.7^2 - \ldots + 2(-7)^n = (1 - (-7)^{n+1})/4$ whenever n is a nonnegative integer.

**Proof:**

Let P(n) be $2\sum_{i=0}^{n}(-7)^i = (1-(-7)^{n+1})/4$, then

**Basis Step:** $2.(-7)^0 = 2$ and

$(1 - (-7)^{0+1})/4 = (1+7)/4 = 2$,

so P(0) is true.

**Inductive Hypothesis:** Assume that P(n) is true.

**Inductive Step:** if P(n+1) is true then prove is done. So P(n+1) is $2\sum_{i=0}^{n+1}(-7)^i$ = $2\sum_{i=0}^{n}(-7)^i + 2.(-7)^{n+1}$ so Using the assumption from the induction hypothesis we have

$$\begin{aligned}P(n+1) &= (1 - (-7)^{n+1})/4 + 2(-7)^{n+1} \\ &= (1 - (-7)^{n+1} + 8(-7)^{n+1})/4 \\ &= (1 + 7(-7)^{n+1})/4 \\ &= (1 - (-7)^{n+2})/4.\end{aligned}$$

Hence, P(n) is true for all nonnegative integers.

**Example 2:**

Prove that 1.1! + 2.2! + … + n.n! = (n+1)! –1, whenever n is a positive integer.

**Proof:**

Let P(n) = 1.1! + 2.2! + … + n.n! = (n+1)! –1, then

**Basis Step:** for n = 1, we have P(1) = 1.1! = 1, Similarly P(1) = (1+1)! –1 = 2-1 =1

Hence P(1) is true.

**Inductive Hypothesis:** Assume that P(n) is true, i.e. 1.1! + 2.2! + … + n.n! = (n+1)! –1.

**Inductive Step:** if we are able to prove that P(n+1) is true then we are done. So we have

P(n+1) = 1.1! + 2.2! + … + n.n! + (n+1)(n+1)!

= (n+1)! –1 + (n+1)(n+1)! (using induction hypothesis)

= (n+1)n! + (n+1)(n+1)! – 1 = (n+1)(n! + (n+1)!) –1

= (n+1)(n! (1+ (n+1)) –1 = (n+1)n! (n+2) –1

= (n + 2)! –1

P(n+1) is true

Hence P(n) is true for all positive integers.

## Strong Induction (Second Principle of Mathematical Induction)

This method uses different inductive step than the first principle. Here we assume that P(k) is true for k = $n_0$, $n_0$ + 1, …., k and show that P(k+1) is true based on the assumption. The steps in this method are:

**Basis Step:** Show P($n_0$) is true.

**Inductive Hypothesis (Strong):** Assume P(k) is true for all $n_0 \leq k \leq n$.

**Inductive Step:** Show based on the assumption that P(k+1) is true.

**Example 1:**

Prove that 3 divides $n^3 + 2n$ whenever n is a nonnegative integer.

**Proof:**

Let P(n) = $n^3 + 2n$, then

**Basis Step:** For n = 0, we have $n^3 + 2n = 0$, this is divisible by 3 hence the statement is true for n = 0.

**Inductive Hypothesis:** assume that the $P(k) = k^3 + 2k$ is divisible by 3 for all nonnegative values for $k \leq n$.

**Inductive Step:** here we are going to show that p(k+1) true. We have

$P(k+1) = (k+1)^3 + 2(k+1) = k^3 +3 k^2 + 3k + 1 + 2k + 2$

$= k^3 + 2k + 3 k^2 + 3k + 3$

$= 3 l + 3 k^2 + 3k + 3$ (since $k^3 + 2k$ is divisible by 3)

$= 3(l + k^2 + k + 1)$

Since both l and k are positive integers $(l + k^2 + k + 1)$ is also positive integer. Hence, P(k+1) is divisible by 3.

So by mathematical induction $n^3 + 2n$ is divisible by three for all nonnegative integers n.

**Example 2:**

Use mathematical induction to show that 1/(2n) ≤ [1.3.5…..(2n –1)]/(2.4…..2n) whenever n is a positive integer.

**Proof:**

Let P(n) be 1/(2n) ≤ [1.3.5…..(2n –1)]/(2.4…..2n)

**Basis Step:** for n =1, we have 1/2n = 1 = [1.3.5…..(2n –1)]/(2.4…..2n), Since 1 ≤ 1, P(1) is true.

**Inductive Hypothesis:** Assume that P(k) is true for all positive k ≤ n.

**Inductive Step:** Now to prove P(k+1) is true we have to show

1/(2(k+1)) ≤ [1.3.5…..(2k –1)(2k + 1)]/(2.4…..2k.2(k+1)) so we have,

1/(2k) . (2k + 1)/(2(k + 1)) ≤ [1.3.5…..(2k –1)(2k + 1)]/(2.4…..2k.2(k+1))

[Above relation is true from inductive hypothesis]

1/(2k).(2k + 1)/(2(k + 1))

= (2k + 1)/(2k).1/(2(k + 1))

= (1 + 1/(2n))1/(2(k + 1))

= 1/(2(k + 1)) + 1/(2(k + 1))(2n)

Here we have,

1/(2(k+1)) ≤ 1/(2(k + 1)) + 1/(2(k + 1))(2n)

≤ [1.3.5…..(2k –1)(2k + 1)]/(2.4…..2k.2(k+1)), hence proved.

## Well Ordering Property

This property states, "Every nonempty set of nonnegative integers has a least element." Using this property we can verify the validity of proofs using mathematical induction.

Using mathematical induction we prove P(1) is true and P(n) → P(n+1) is true for all positive integers n. If the proof by mathematical induction is not valid then P(n) is true for all positive integers n would be false. Let the set of positive integers for which P(n) is false be T. then T is nonempty since there is at least one element in T such that P(n) is false. By the well ordering property, T has a least element, let the least element be k. we know that m cannot be 1 because we have already proved that P(1) is true. So k is a positive integer greater than 1 so k –1 is a positive integer, so we have P(k-1) must be true. Here k –1 is less than k i.e. k-1 is not in the set T. Since the implication P(k-1) → P(k) is also true, P(k) must be true. This contradicts the choice of k. Hence, P(n) must be true for all positive integers n.

**Remember!!! You may prove wrongly if you do not take care**

Prove $a^n = 1$ for all nonnegative integers n, whenever a is a nonzero real number.

**Proof:**

**Basis Step:** for n = 0, $a^0 = 1$ by the definition of $a^0$.

**Inductive Hypothesis:** assume that $a^k = 1$ for all nonnegative integers $k \leq n$.

**Inductive Step:** we have $a^{k+1} = a^k . a^k / a^{k-1} = 1.1/1 =1$.

Hence proved.

**Attention:**

Whenever k + 1 = 1 the above proof fails because here k = 0 so that $a^{k+1} = a^k . a^k / a^{k-1} = a^0 . a^0 / a^{-1} = ?$. Here we cannot get the value for denominator from previously obtained value. So choosing base n = 0 does not produce correct result for n = 1 but mathematical induction says that P(0) → P(1) which is not true here. Similarly choosing base n =1 disprove the statement at basis step.

# Recursive Definition

The process of defining the object in terms of itself is called recursion. Such a way of representation is given by recursive definition. For e.g. natural numbers can be defined in terms of itself as $N_n = N_{n-1} +1$, for $N_0 = 0$ and n = 0, 1, 2, ….

# Recursively Defined Functions, Sets and Structures

When we try to define a function recursively, where the domain of the function is set on nonnegative integers, we define such a function through two steps:

**Basis Step:** Specify the value of the function at base (base is generally 0 or 1). This is generally well known value of the function at the lowest value of integer.

**Recursive Step:** Specify the rule for finding the value of a function by using the value of a function already found i.e. at first base case is used and next result obtained from function definition that uses base case, and so on.

This kind of definition is also called **inductive definition**.

Similarly if you want to define sets or structures then the similar two steps above is used. You may also put exclusion rule in recursive step such that the elements of the sets are specified.

**Example 1:**

Give a recursive definition of a sequence $\{a_n\}$, n =1, 2, …, n if $a_n = 10^n$.

**Solution:**

**Basis Step:** $a_1 = 10^1 = 10$.

**Recursive Step:** $a_n = 10a_{n-1}$. This is the recursive definition required.

**Example 2:**

Give a recursive definition of the set of even positive integers.

**Solution:**

Let E be the set of even positive integers.

**Basis Step:** $2 \in E$

**Recursive Step:** If $a \in E$, then $a + 2 \in E$.

The above recursive definition gives a set of even positive integers.

*Note: To prove that the recursive definition is correct we can use mathematical induction principle.*

**Example 4:**

Show that $f_1^2 + f_2^2 + \ldots + f_n^2 = f_nf_{n+1}$,whenever n is a positive integer. Here $f_i$'s are $i^{th}$ fibonacci numbers (see book for more details on fibonacci numbers).

**Proof:**

Let P(n) be $f_1^2 + f_2^2 + \ldots + f_n^2 = f_nf_{n+1}$.

**Basis Step:** $P(1) = f_1^2 = 1^2 = 1.1 = f_1f_2$. So P(1) is true.

**Inductive Hypothesis:** Assume that P(k) is true for all positive integers $k \le n$.

**Inductive Step:** We have

$P(k+1) = f_1^2 + f_2^2 + \ldots + f_{k+1}^2$

$= f_kf_{k+1} + f_{k+1}^2$

$= f_{k+1}(f_k + f_{k+1})$

$= f_{k+1}f_{k+2}$. [$f_k + f_{k+1}= f_{k+2}$, this is fibonacci numbers property]

Hence P(k+1) is true.

So by mathematical induction P(n) is true for all positives integers n.

**Theorem 1(Lame's Theorem):** Let a and b be positive integers with $a \ge b$ then number of divisions used by the Euclidean algorithm to find gcd(a,b) is less than or equal to five times the number of decimal digits in b.

**Proof:**

Euclidean algorithm for finding gcd(a, b) with $a \ge b$ gives the following sequence of equations.

$r_0 = r_1q_1 + r_2$. $0 \le r_2 < r_1$. [Here $r_0 = a$ and $r_1 = b$]

$r_1 = r_2q_2 + r_3$. $0 \le r_3 < r_2$.

$\vdots$

$r_{n-2} = r_{n-1}q_{n-1} + r_n$. $0 \le r_n < r_{n-1}$.

$r_{n-1} = r_nq_n$.

The gcd(a, b) = $r_n$ and n divisions are used for finding it. All the quotients $q_i$, for i =1, 2,…n all at least 1. We have $q_n \geq 2$, since $r_n < r_{n-1}$. So we have

$$r_n \geq 1 = f_2.$$
$$r_{n-1} \geq 2\, r_n \geq 2f_2 = f_3.$$
$$r_{n-2} \geq r_{n-1} + r_n \geq f_3 + f_2 = f_4.$$
$$\vdots$$
$$r_2 \geq r_3 + r_4 \geq f_{n-1} + f_{n-2} = f_n.$$
$$b = r_1 \geq r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1}.$$

From the above relations we can conclude that if n divisions are used by the Euclidean algorithm to find gcd(a, b) with $a \geq b$ then $b \geq f_{n+1}$. We have $f_{n+1} > \phi^{n-1}$ for $n > 2$, where $\phi = (1 + \sqrt{5})/2$ (prove using mathematical induction). So we have $b > \phi^{n-1}$.

Now taking log on both sides, $\log_{10}b > (n-1)\log_{10}\phi$ but since $\log_{10}\phi \approx 0.208 > 1/5$, we have $\log_{10}b > (n-1)/5$ i.e. $(n-1) < 5 \log_{10}b$. If we know that the b has m decimal digits, then we have $b < 10^m$ and $\log_{10}b < m$. Here $(n-1) < 5m$, and since m is an integer, $n \leq 5m$. This is the proof.

# Structural Induction

While proving the recursively defined sets we use a form of mathematical induction called structural induction. This method consists two parts.

**Basis Step:** Show that the result holds for all elements specified in the basis step of the recursive definition to be in the set.

**Recursive Step:** Show that if the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the result holds for these new elements.

### Validity of Structural Induction

The validity of structural induction can be seen as the validity of the mathematical induction. If P(n) denotes the statement that is recursively defined, for all positive integers n. The basis step of the structural induction method correspondence to the basis step of the mathematical induction method. We can see that the recursive step in the structural induction tells if P(k) is true it implies P(k+1), where P(k) is assumed already and the P(k+1) is derived in terms of P(k). Hence it follows the proofs by mathematical induction.

**Example:**

Recursive definition of the set of leaves and the set of internal vertices of a full binary tree can be defined as:

**Basis Step:** The root r is a leaf of the full binary tree with exactly one vertex r. This tree has no internal vertices.

**Recursive Step:** The set of leaves of the tree $T = T_1.T_2$ is the union of the set of the leaves of $T_1$ and the set of leaves of $T_2$. The internal vertices of T are the root r of T and the union of the set of internal vertices of $T_1$ and the set of internal vertices of $T_2$.

Use structural induction to show that l(T), the number of leaves of a full binary tree T, is 1 more than i(T), the number of internal vertices of T.

**Proof:**

**Basis Step:** Root r of a full binary tree has only one vertex and that is leaf of the tree. So $l(T) = 1$ and $i(T) = 0$, hence clearly T contains number of leaves 1 greater than number of internal vertices i.e. $l(T) - i(T) = 1$.

**Recursive Step:** Assume that $T_1$ and $T_2$ are trees holding the property $l(T_1) – i(T_1) = 1$ and $l(T_2) – i(T_2) = 1$. To complete the proof we must show that $l(T) – i(T) = 1$, where $T = T_1.T_2$. We know that $l(T) = l(T_1) + l(T_2)$ [form the recursive definition] and $i(T) = 1 + i(T_1) + i(T_2)$ [from the recursive definition]. So,

$$l(T) – i(T) = l(T_1) + l(T_2) – 1 - i(T_1) - i(T_2).$$
$$= l(T_1) - i(T_1) + l(T_2) - i(T_2) – 1.$$
$$=1 + 1 – 1 \text{ [from assumption above] } = 1$$

Hence the proof.

# Recursive Algorithms

An algorithm is recursive it solves the problem by reducing the size of the same problem using smaller input size. In this section few recursive algorithms are presented.

**Example 1:**

Give the recursive algorithm for finding the sum of the first n positive integers.

**Solution:**

**Input:** A positive integer n.

**Output:** the sum of positive integers form 1 up to n.

```
PositiveInteger nsum(PositiveInteger n)
{
if(n = =1) then return 1;
else  return  nsum(n-1) + n;
}
```

**Example 2:**

Devise a recursive algorithm for finding $x^n$**mod**m whenever n, x, and, m are positive integers based on the fact that $x^n$**mod**m = ($x^{n-1}$**mod**m.x**mod**m) **mod**m.

**Solution:**

**Input:** Three positive integers n, x, and m.

**Output:** $n^{th}$ x modulo m.

```
PositiveInteger nmod(n, x, m)
{
if n = = 1 then return xmodm;
else return ((nmod(n-1, x, m).xmodm)modm.
}
```

*Note: Try to understand difference between use of recursion and iteration*

# Self Studies

Read chapter 1 and 3 of your textbook such that you can cover all the read materials in the class.