Module 2:

Fundamentals of Logic *contd*.:

- The Use of Quantifiers, Quantifiers,
- Definitions and the Proofs of Theorems,

Properties of the Integers:

- Mathematical Induction,
- The Well Ordering Principle
- Mathematical Induction,
- Recursive Definitions.

Fundamentals of Logic *contd*.:

Qua ntifiers:

Given a predicate P (x), the statement "for some x, P (x)" (or "there is some x such that p(x)"), represented "∃x P (x)", has a definite truth value, so it is a proposition in the usual sense. For instance if P (x) is "x + 2 = 7" with the integers as

universe of discourse, then ∃x P (x) is true, since there is indeed an integer, namely 5, such that P (5) is a true statement. However, if

Q(x) is "2x = 7" and the universe of discourse is still the integers, then ∃x Q(x) is false. On the other hand, ∃x Q(x) would be true if we extend the universe of discourse to the rational numbers. The symbol
∃ is called the existential quantifier.

Analogously, the sentence "for all x, P (x)"—also "for any x, P (x)", "for every x, P (x)",

"for each x, P (x)"—, represented "∀x P (x)", has a definite truth value. For instance, if P (x) is "x + 2 = 7" and the

universe of discourse is the integers, then ∀x P (x) is false. However if Q(x) represents "$(x + 1)^2 = x^2 + 2x + 1$" then ∀x Q(x) is true. The symbol ∀ is called the universal quantifier.

In predicates with more than one variable it is possible to use several quantifiers at the same time, for instance ∀x∀y∃z P (x, y, z), meaning "for all x and all y there is some z such that P (x, y, z)".

Note that in general the existential and universal quantifiers cannot be swapped, i.e., in general ∀x∃y P (x, y) means something different from ∃y∀x P (x, y). For instance if x and y represent human beings and P (x, y) represents "x is a friend of y", then ∀x∃y P (x, y) means that everybody is a friend of someone, but ∃y∀x P (x, y) means that there is someone such that everybody is his or her friend.

A predicate can be partially quantified, e.g. ∀x∃y P (x, y, z, t). The variables quan tified (x and y in the example) are called bound variables, and the rest (z and t in the example) are called free variables. A partially quantified predicate is still a predicate, but depending on fewer variables.

Proofs

M ath ematic al Sy st ems, Proofs:

A Mathematical Sys- tem consists of:

1. Axioms : propositions that are assumed true.
2. Definitions : used to create new concepts from old ones.
3. Undefined terms : corresponding to the primitive concepts of the system (for instance in set theory the term “set” is undefined).

A theorem is a proposition that can be proved to be true. An argument that establishes the truth of a proposition is called a proof.

Example : Prove that if $x > 2$ and $y > 3$ then $x + y > 5$.

Answer : Assuming $x > 2$ and $y > 3$ and adding the inequalities term by term we get: $x + y > 2 + 3 = 5$.

That is an example of direct proof. In a direct proof we assume the hypothesis together with axioms and other theorems previously proved and we derive the conclusion from them.

An indirect proof or proof by contrapositive consists of proving the contrapositive of the desi red impli cation, i.e., instead of proving $p \rightarrow q$ we prove $\neg q \rightarrow \neg p$.

Example : Prove that if $x + y > 5$ then $x > 2$ or $y > 3$.

Answer : We must prove that $x + y > 5 \rightarrow (x > 2)$ � $(y > 3)$. An indirect proof consists of proving $\neg((x > 2)$ � $(y > 3)) \rightarrow \neg(x + y > 5)$. In fact: $\neg((x > 2)$ � $(y > 3))$ is the same as $(x \le 2)$ �$(y \le 3)$, so adding both inequalities we get $x + y \le 5$, which is the same as $\neg(x + y > 5)$.

Proof by Contradiction. In a proof by contradiction or (Reductio ad Absurdum) we assume the hypotheses and the negation of the conclu- sion, and try to derive a contradiction, i.e., a proposition of the form r � $\neg r$.

Example : Prove by co ntradiction that if $x + y > 5$ then either $x > 2$ or $y > 3$.

Answer : We assume the hypothesis $x + y > 5$. From here we must conclude that $x > 2$ or $y > 3$. Assume to the contrary that “$x > 2$ or $y > 3$” is false, so $x \le 2$ and $y \le 3$. Adding those inequalities we get $x \le 2 + 3 = 5$, which contradicts the hypothesis $x + y > 5$. From here we conclude that the assumption “$x \le 2$ and $y \le 3$” cannot be right, so “$x > 2$ or $y > 3$” must be true.

Remark : Sometimes it is difficult to distinguish between an indirect proof and a proof by contradiction. In an indirect proof we prove an implication of the form $p \to q$ by proving the contrapositive $\neg q \to \neg p$. In an proof by contradiction we prove an s (which may or may not be an implication) by assuming $\neg s$ and contradiction. In fact proofs by contradiction are more general than indirect proofs.

Exerc CSE : Prove by contradiction that 2 is not ~~a~~ rational number, i.e., there are no integers a, b such that 2 = a/b.

Answer : Assume that 2 is rational, i.e., 2 = a/b, where a and b are integers and the fraction is written in least terms. Squaring both sides we have $2 = a^2/b^2$, hence $2b^2 = a^2$. Since the left hand side is even, then a^2 is even, but this implies that a itself is even, so $a = 2a^!$. Hence: $2b^2 = 4a^{!2}$, and simplifying: $b^2 = 2a^{!2}$. This implies that b^2 is even, so b is even: $b = 2b^!$. Consequently $a/b = 2a^!/2b^! = a^!/b^!$, contradicting the hypothesis that a/b was in least terms.

Arguments, Ru les of I nfe rence:

An argument is a se- quence of propositions $p_1, p_2, \ldots, p_n$ called hypotheses (or premCSEs) followed by a proposition q called conclusion. An argument is usually written:

p_1

p_2

.

p_n

� q

or

$p_1, p_2, \ldots, p_n$ / � q

The argument is called valid if q is true whenever $p_1, p_2, \ldots, p_n$ are true; otherwCSE it is called invalid.

Rules of inference are certain simple arguments known to be valid and used to make a proof step by step. For instance the following argument is called modus ponens or rule of detachment :

$p \to q$ p

�q

In order to check whether it is valid we must examine the following truth table:

p	q	p	→ p	q	
T	T	T	T	T	
T	F	F	T	F	
F	T	T	F	T	
F	F	T	F	F	

If we look now at the rows in w hich both p → q and p are true (just the first row) we see that also q is true, so the argument is val id.

Other rules of inference are the following:

1. *Modus Ponens* or *Rule of Detachment*:

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

2. *Modus Tollens*:

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

3. *Addition*:

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

4. *Simplification*:

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

5. *Conjunction*:

Arguments are usually written using three columns. Each row con- tains a label, a statement and the reason that justifies the introduction of that statement in the argument. That justification can be one of the following:

1. The statement is a prem CSE.
2. The statement can be derived from statements occurring earlier in the argument by using a rule of inference.

Example : Consider the following statements: “I take the bus or I walk. If I walk I get tired. I do not get tired. Therefore I take the bus.” We can formalize this by calling B = “I take the bus”, W = “I walk” and T = “I get tired”. The premCSEs are B

�W , W → T and

¬T , and the conclusion is B. The argument can be described in the following steps:

step	statement	reason
1)	W → T	
2)	¬T	PremCSE
3)	¬W	1,2, Modus Tollens
4)		Prem CSE
5)	B � W	4,3, Disjunctive Syllogism
	� B	

Quantified Statements:

We state the rules for predicates with one variable, but they can be gener- alized to pre dicates with two or more variables.

1. Universal Instantiation. If �x p(x) is true, then p(a) is true for each specific element a in the universe of discourse; i.e.:

�x p(x)

� p(a)

For instance, from �x (x + 1 = 1 + x) we can derive 7 + 1 = 1 + 7.

2. Existential Inst antia tion. If �x p(x) is true, then p(a) is true for some specific element a in the universe of discourse; i.e.:

�x p(x)

� p(a)

The difference respect to the previous rule is the restriction in the meaning of a, which now represents some (not any) element of the universe of discourse. So, for instance, from �x (x^2 = 2) (the universe of discourse is the real numbers) we derive the existence of some element, which we may represent $\pm\sqrt{2}$, such that $(\pm\sqrt{2})^2 = 2$.

3. Universal Generalization. If p(x) is proved to be true for a generic element in the universe of discourse, then �x p(x) is true; i.e.:

$$\frac{p(x)}{\therefore\ \forall x\, p(x)}$$

� �x p(x)

By "generic" we mean an element for which we do not make any assumption other than its b elonging to the universe of discourse. So, for instance, we can prove �x $[(x + 1)^2 = x^2 + 2x + 1]$ (say, for real numbers) by assuming that x is a generic real number and using algebra to prove $(x + 1)^2 = x^2 + 2x + 1$.

4. E xistential Generalization. If p(a) is true for some specific ele- ment a in the universe of discourse, then �x p(x) is true; i.e.:

p(a)

x p(x)

For instance: from 7 + 1 = 8 we can derive �x (x + 1 = 8).

Example : Show that a counterexample can be used to disprove a universal statement, i.e., if a is an element in the universe of discourse,

then from ¬p(a) we can derive ¬�x p(x). An swer : The argument is as follows:

step	statement	reason
1)	¬p(a)	Prem CSE
2)	�x ¬p(x)	Existential Generalization
3)	¬�x p(x)	Negation Universal Statement

Properties of the Integers

MATHEMA TICAL INDUCTION:

The method of mathematical induction is based on a principle called the induction principle .

I NDUCTION PRINCIPLE:

The induction principle states as follows : let S(n) denote an open statement that involves a positive integer n .suppose that the following conditions hold ;

1. S(1) is true
2. If whenever S(k) is true for some particular , but arbitrarily chosen k $€Z^+$, then S(k+1) is true. Then S(n) is true for all n € Z+ . Z+ denotes the set of all positive integers .

Suppose we wish to prove that a certain statement S(n) is true for all integers n ≥1 , the

method of proving such a statement on the basis of the induction principle is calledd the method of mathematical induction. This method consist of the following two steps, re spectively called the basis step and the induction step

1) Basis step: verify that the statement S(1) is true ; i.e. verify that S(n) is true for n=1.
2) Induction step: assuming that S(k) is true , where k is an integer≥1, show that S(k+1) is true.

Many properties of positive integers can be proved by mathematical induction.

Principle of Mathematical Induction:

Let P be a prop- erty of positive integers such that:

1. Basis Step: P (1) is true, and
2. Inductive Step: if P (n) is true, then P (n + 1) is true. Then

P (n) is true for all positive integers.

Remark : The prem CSE P (n) in the inductive step is called Induction Hypothesis.

The validity of the Principle of Mathematical Induction is obvious. The basis step states that P (1) is true. Then the inductive step implies that P (2) is also true. By the inductive step again we see that P (3) is true, and so on. Consequently the property is true for all positive integers.

Remark : In the basis step we may replace 1 with some other integer m. Then the

conclusion is that the property is true for every integer n greater than or equal to m.

Example : Prove that the sum of the n first odd positive integers is n^2, i.e., 1 + 3 + 5 + ••• + (2n — 1) ‘ n^2.

Answer : Let S(n) ‘ 1 + 3 + 5 + ••• + (2n — 1). We w ant to prove by induction that for every positive integer n, S(n) ‘ n^2.

1. Basis Step: If n ‘ 1 we have S(1) ‘ 1 ‘ 1^2, so the property is true for 1.
2. Inductive Step: Assume (Induction Hypothesis) that the prop- erty is true for some positive integer n, i.e.: S(n) ‘ n^2. We must prove that it is also true for n + 1, i.e., S(n + 1) ‘ $(n + 1)^2$. In fact:

S(n + 1) ‘ 1 + 3 + 5 + ••• + (2n + 1) ‘ S(n) + 2n + 1 .

But by induction hypothesis, S (n) ‘ n^2, hence:

S(n + 1) ‘ n^2 + 2n + 1 ‘ $(n + 1)^2$.

This completes the induction, and shows that the property is true for all positive integers.

Example : Prove that 2n + 1 ≤ 2^m for n ≥ 3.

Answer : This is an example in which the property is not true for all positive integers but only for integers greater than or equal to 3.

1. Basis Step: If n ‘ 3 we have 2n + 1 ‘ 2 • 3 + 1 ‘ 7 and 2^m ‘ 2^3 ‘ 8, so the property is true in this case.

2. Inductive Step: Assume (Induction Hypothesis) that the prop- erty is true for some positive integer n, i.e.: 2n + 1 ≤ 2^m . We must prove that it is also true for n + 1, i.e., 2(n + 1) + 1 ≤ 2^{m+1} . By the induction hypothesis we know that 2n ≤ 2^m , and we also have that 3 ≤ 2^m if n ≥ 3, hence

2(n + 1) + 1 ‘ 2n + 3 ≤ $2^m + 2^m$ ‘ 2^{m+1} .

This completes the induction, and shows that the property is true for all n ≥ 3.

Exerc CSE : Prove the following identi ties by induction:

n (n + 1)
• 1 + 2 + 3 + •• • + n ‘ ______ .
2n (n + 1) (2n + 1)
• $1^2 + 2^2 + 3^2$ + • • • + n^2 ‘ ______ 6 .

• $1^3 + 2^3 + 3^3$ + ••• + n^3 ‘ $(1 + 2 + 3 + \cdots + n)^2$.

Strong Form of M athemati cal Induct ion:

Let P be a property of positive integers such that:

1. Basis Step: P (1) is true, and

2. Inductive Step: if P (k) is true for all 1 ≤ k ≤ n then P (n + 1) is true.

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

Example : Prove that every integer n ≥ 2 is prime or a product of primes. Answer :

1. Basis Step: 2 is a prime number, so the property holds for n ‘ 2.
2. Inductive Step: Assume that if 2 ≤ k ≤ n, then k is a prime number or a product of primes. Now, either n + 1 is a prime number or it is not. If it is a prime number then it verifies the property. If it is not a prime number, then it can be written as the product of two positive integers, n + 1 = k_1 k_2, such that 1 < k_1, k_2 < n + 1. By induction hypothesis each of k_1 a nd k_2 must be a prime or a product of primes, hence n + 1 is a product of primes.

This completes the proof.

The W ell-Orde ring Pr inci ple

Every nonempty set of positive integers has a smallest element.

Example : Prove that √2 is irrational (i.e., √2 cannot be written as a quotient of positive integers) using the well-ordering principle.

Hence starting with a fractional representation of 2 ‘ a/b we end up with another fractional representation 2 ‘ b/a! with a smaller numerator b < a. Repeating the same argument with the fraction b/a! we getanother fraction with an even smaller numerator, and so on. So the set of possible numerators of a fraction representing √ cannot have a smallest contra dicting the well-ordering principle. Consequently, our assumption that √ 2 is rational has to be false.

Reccurence relations

Here we look at recursive definitions under a d ifferent point of view. Rather than definitions they will be considered as equations that we must solve. The point is that a recursive definition is actually a def- inition when there is one and only one object satisfying it, i.e., when the equations involved in that definition have a unique solution. Also, the solution to thoseequations may provide a closed-form (explicit) formula for the object defined.

The recursive step in a recursive definition is also called a recurrence relation. We will focus on kth-order linear recurrence relations, which are of the form

$C_0 x_m + C_1 x_{m-1} + C_2 x_{m-2} + \cdots + C_k x_{m-k}$ ‘ b_m ,

where C_0 ‘ O. If b_m ‘ O the recurrence relation is called homogeneous. OtherwCSE it is called non-homogeneous.

The basis of the recursive definition is also called initial conditions of the recurrence. So, for instance, in the recursive definition of the Fibonacci sequence, the recurrence is

F_m ‘ $F_{m-1} + F_{m-2}$

or

$F_m — F_{m-1} — F_{m-2}$ ‘ O ,

and the initial conditions are

F_0 ‘ O, F_1 ‘ 1 .

One way to solve some recurrence relations is by iteration, i.e., by using the recurrence repeatedly until obtaining a explicit close-form formula. For instance consider the following recurrence relation:

x_m ‘ r x_{m-1} (n > O) ; x_0 ‘ A .

By using the recurrence repeatedly we get:

x_m ‘ r x_{m-1} ‘ r^2 x_{m-2} ‘ r^3 x_{m-3} ‘ • • • ‘ r^m x_0 ‘ A r^m ,

hence the solution is x_m ‘ A r^m .

Example : Assume that a country with currently population growth rate (birth rate minus death rate) of 1% per year, and it also receives 1OO thousand i mmigrants per year (which are quickly assimilated and reproduce at the same rate as the native population). Find its population in 1O years from now. (Assume that all the immigrants arrive in a single batch at the end of the year.)

Answer : If we call x_n ‘ population in year n from now, we have:

x_n ‘ 1.O1 x_{n-1} + 1OO, OOO (n > O); x_0 ‘ 1OO, OOO, OOO .

This is the equation above with r ‘ 1.O1, c ‘ 1OO, OOO and A ‘ 1OO, OOO, OO, hence:

$$\frac{1.O1^n - 1}{1.O1 - 1}$$

x_n ‘ 1OO, OOO, OOO • $1.O1^n$ + 1OO, OOO

‘ 1OO, OOO, OOO • $1.O1^n$ + 1OOO ($1.O1^n$ — 1) .

So: 462, 317 .

The second particular case is for r ‘ 1 and c_m ‘ c + d n, where c and d are constant (so c_m is an arithmetic sequence):

x_m ‘ x_{m-1} + c + d n (n > O) ; x_0 ‘ A .

The solution is now

$$x_m \text{ ‘ } A + \sum_{k=1}^{m} (c + d\,k) \text{ ‘ } A + c\,n + \frac{d\,n\,(n+1)}{2} .$$

Second Order Recurrence Relations.

relation

$$C_0\,x_m + C_1\,x_{m-1} + C_2\,x_{m-2} \text{ ‘ } O .$$

First we will look for solutions of the form x_m ‘ c r^m . By plugging in the equation we get:

$$C_0\,c\,r^m + C_1\,c\,r^{m-1} + C_2\,c\,r^{m-2} \text{ ‘ } O ,$$

hence r must be a solution of the following equation, called the characteristic equation of the recurrence:

$$C_0 r^2 + C_1 r + C_2 = 0 .$$

Let r_1 , r_2 be the two (in general complex) roots of the above equation. They are called characteristic roots. We distinguish three cases:

1. Distinct Real Roots. In this case the general solution of the recurrence relation is

$$x_m = c_1 r_1^m + c_2 r_2^m ,$$

where c_1 , c_2 are arbitrary constants.

2. Double Real Root. If $r_1 = r_2 = r$, the general solution of the recurrence relation is

$$x_m = c_1 r^m + c_2 n r^m ,$$

where c_1 , c_2 are arbitrary constants.

3. Complex Roots. In this case the solution could be expressed in the same way as in the case of distinct real roots, but in order to avoid the use of complex numbers we write $r_i = r e^{\alpha i}$,

$r_2 = r e^{-\alpha i}$, $k_i = c_i + c_2$, $k_2 = (c_i - c_2)$ i, which yields:

$$x_m = k_i r^m \cos n\alpha + k_2 r^m \sin n\alpha .$$

RE CURSIVE DEFINITIONS:

RECURRENCE RELAT IONS:- The important methods to express the recurrance formula in explict form are

1) BACKTRACKING METHOD
2) CHARACTERISTIC EQUATION METHOD

BACKTRACKING METHOD:

This is suitable method for linear non-homogenous recurrence relation of the type

$$x_n = r\, x_{n-1} + s$$

The general method to find explicit formula

$x_n = r^{n-1} x_1 + s(r^{n-1}-1)/(r-1)$ where $r\neq1$ is the general explicit

CHARACTERISTIC EQUATION METHOD:

This is suitable method to find an explicit formula for a linear homogenous recurrance relation

LINEAR HOMOGENOUS RELATION :

A recurrence relation of the type $a_n = r_1 a_{n-1} + r_2 a_{n-2} + \ldots\ldots + r_k a_{n-k}$ where r_i 's' are constants is a linear ho mogenous recurrence relation (LHRR) of degree k

1) A relation $c_n = -2 c_{n-1}$ is a LHRR of degree 1 .
2) A relation $x_n = 4 x_{n-1} + 5$ is a linear non HRR because 2nd term in RHS is a constant . It doesn't contain x_{n-2} factor .
3) A relation $x_n = x_{n-1} + 2x_{n-2}$ is a LHRR of degree 2

4) A relation $x_n = x^2_{n-1} + x_{n-2}$ is a non linear , non HRR because the 1st term in RHS is a second degree term.

CHARACTERISTIC EQUATION:

$a_n = r_1 a_{n-1} + r_2 a_{n-2} + \ldots\ldots + r_k a_{n-k}$..(1) is a LHRR of degree K . $x^k = r_1 x^{k-1} + r_2 x^{k-2} + \ldots. + r_k$ is called characteristic equation.

- Let $a_n = r_1 a_{n-1} + r_2 a_{n-2}$ be LHRR of degree 2. its characteristic equation is $x^2 = r_1 x + r_2$ or $x^2 - r_1 x - r_2 = 0$. if the characteristic equation has 2 distinct roots e_1 , e_2 then the explicit formula of the recurrence relation in $a_n = u\, e^n{}_1 + v\, e^n{}_2$ where u and v depends on the initial values.

- Let $a_n = r_1 a_{n-1} + r_2 a_{n-2}$ be a LHRR of degree 2 . Its characteristic equation is $x^2 - r_1 x - r_2 = 0$ if the characteristic equation has repeated roots e, then the explicit formula is $a_n = u\, e^n + v\, n\, e^n$ where u and v depends on the initial values.