Discrete Structures

Week-03-Lecture # 02

Mr. Hafiz Tayyeb Javed

Department of Computer Science

FAST -- National University of Computer and

Emerging Sciences. CFD Campus

Q-1 Infer new rules

Assume,

RK= Reading the newspaper in the kitchen.

GK= Glasses are on the kitchen table.

SB= I saw my glasses at breakfast.

RL= Reading the newspaper in the living room.

GC= Glasses are on the coffee table.

So by rules of inference,

❑ Example: You are about to leave for University in the morning and discover that you don't have your glasses. You know the following statements are true.

A. If I was reading the newspaper in the kitchen, then my glasses are on the kitchen table.

B. If my glasses are on the kitchen table, then I saw them at breakfast.

C. I did not see my glasses at breakfast.

D. I was reading the newspaper in the living room or I was reading the newspaper in the kitchen.

E. If I was reading the newspaper in the living room then my glasses are on the coffee table.

Where are the glasses?? Deduct some rules using inference rules

Inference Rule -- Application – An Example

Assume, RK= Reading the newspaper in the kitchen.

GK= Glasses are on the kitchen table.

SB= I saw my glasses at breakfast.

RL= Reading the newspaper in the living room.

GC= Glasses are on the coffee table.

So by rules of inference,

1.
$$\frac{\begin{array}{ll} RK \rightarrow GK & (by\ A) \\ GK \rightarrow SB & (by\ D) \end{array}}{\therefore RK \rightarrow SB\ (Transiticity)}$$

2.
$$\frac{\begin{array}{ll} RK \rightarrow SB & (by\ 1) \\ \sim SB & (by\ C) \end{array}}{\therefore \sim RK\ \ (by\ modus\ tollens)}$$

3.
$$\frac{\begin{array}{ll} RL \veebar RK & (by\ D) \\ \sim RK & (by\ 2) \end{array}}{\therefore RL\ \ \ (by\ elimination)}$$

4.
$$\frac{\begin{array}{ll} RL \rightarrow GC & (by\ C) \\ RL & (by\ 3) \end{array}}{\therefore GC\ \ \ (by\ modus\ ponens)}$$

So the Glasses are on the Coffee table.

Predicate Logic

- Can be considered as a model to investigate certain arguments that cannot be expressed in propositional logic.

- Given the following propositions as premises
  - All human beings are mammals
  - Peter is a human being

  We should be able to conclude that
  - Peter is a mammal.

- This raises two questions
  - How to express propositions like the first premise?
  - How to provide rules to help judge the validity of the argument?

Predicate Logic

- In propositional logic we may state.

- "Peter is a human being"

  and

  - "Ann is a human being"

- But we have no means to express that the two propositions are about the same property: "**Is a human being**"

Predicate Logic

- A predicate p(x) describes a property, say "x" is a human being.

  where x is a free variable that may be substituted by values in the **Universe of discourse** (UOD also called domain) of the predicate.

- For Example, we can write the two propositions on the previous slide as: p(peter) and p(Ann).

Predicates

Statements involving variables, such that

"X > 3", "X = Y+3", "X + Y = Z"

and

"Computer X is under attack by an intruder"

and

"Computer X is functioning properly"

Predicates

- These statements are neither true nor false

- When variables are substituted by values (elements) in the domain, the resulting statement is either true or false.

- The set of all such elements that make the predicate true is called the truth set of the predicate.

Predicates

- For example

  - Let p(X) denote X>3,
    - What are the truth values of p(4) and p(2)?

  - P(4), set X = 4,

  - ⇒ 4 > 3, **Which is true**.

  - P(2), set X = 2,

  - ⇒ 2 > 3, **Which is false**.

The Universal Quantifier

- One sure way to change predicated into statements is to assign specific values to all their variables.

- Another way is to add quantifiers. Words that refer to quantities such as "some" or "all"

- The symbol ∀ denotes "for all" and is called the **<u>universal quantifier</u>**.

- Other expressions: For every, for arbitrary, for any, for each, given any.

The Universal Quantifier

- Let Q(x) be a predicate and D the domain of x
- Universal statement is a statement of the form

$$\forall x \in D, Q(x)$$

- True if and only if Q(x) is true for every x in D.

- False if and only if Q(x) is false for at least one x in D

- Value of x for which Q(x) is false is called Counterexample.

The Universal Quantifier

❑ **Example:** Truth and falsity of Universal Statement.

- Let D = {1, 2, 3, 4, 5}, and consider the statement

$$\forall x \in D, x^2 \geq x$$

Show that the statement is true.

- Consider the statement $\forall x \in \boldsymbol{R}, x^2 \geq x$

Find a counterexample to show that this statement is false.

❑ **Solution:** Check that "$x^2 \geq x$" is true for each individual x in D.

$$1^2 \geq 1, \ 2^2 \geq 2, \ 3^2 \geq 3, \ 4^2 \geq 4, \ 5^2 \geq 5$$

Hence "$\forall x \in D, x^2 \geq x$" is true.

Counterexample: Take $x = \frac{1}{2}$, then x is in $\boldsymbol{R}$ (since $\frac{1}{2}$ is a real number) and

$$\left(\frac{1}{2}\right)^2 = \frac{1}{4} \quad \frac{1}{2}$$

Hence "$\forall x \in \boldsymbol{R}, x^2 \geq x$" is false.

The Existential Quantifier

❑   The symbol ∃ denotes "There Exists".

For Example: The sentence "There is a student in Math" can be written as

"∃ a person p such that p is a student in Math"

Or more Formally

"∃ $p \in P$ such that p is student in math"

Other Expressions:

There is a , we can find a, there is at least one, for some, for at least one.

The Existential Quantifier

Let Q(x) be the predicate, and D the domain of x.

An existential statement is a statement of the form,

$$\text{``} \exists \, p \in P \text{ such that Q(x)''}$$

True, if and only if, Q(x) is true for at least one x in D.

False, if and only if, Q(x) is false for all x in D.

The Existential Quantifier

❑ **Example:** Truth and falsity of Existential Statement.

- Consider the statement

$$\exists\, m \in Z^+, \text{such that } m^2 = m$$

Show that the statement is true.

- Let E= [5, 6, 7, 8] and consider the statement

$$\exists\, m \in E, \text{such that } m^2 = m$$

Show that this statement is false.

❑ **Solution:**

- Observe that $1^2 = 1$. Thus $m^2 = m$ is true for at least on integer m. hence "$\exists\, m \in Z$ such that $m^2 = m$ is true.

- Note that $m^2 = m$ is not true for any integers m form 5 through 8:

$$5^2 = 25 \neq 5,\, 6^2 = 36 \neq 6,\, 7^2 = 49 \neq 7,\, 8^2 = 64 \neq 8$$

Hence "$\exists\, m \in E$, such that $m^2 = m$" is false.

Universal Conditional Statement

Probably, the most important form of statement

$$\forall x, \text{if } P(x) \text{ then } Q(x).$$

❑ **Example:**

- $\forall x \in \boldsymbol{R}, \text{if } x > 2 \text{ then } x^2 > 4$
- Whenever a real number is greater than 2, its square is greater than 4.

OR

- The square of any real number greater than 2 is greater than 4.

- Translating sentences in English into logical expression is crucial task in mathematics, logic, programming, artificial intelligence, and many other disciplines.

Equivalent forms of Universal Statement

∀ x ∈ U, if P(x) then Q(x). Can always be written as

∀ x ∈ D , Q(x)   By narrowing U to D consisting of all values of x that make P(x)true

❑ **Example:**

- ∀ real numbers x, if x is an integer then x is rational. Means the same as
- ∀ integers x, x is rational.

∀ x ∈ **R** if P(x) then Q(x)	P(x) = x is an integer
∀ x ∈ Z, Q(x)	Q(x) = x is rational

Equivalent forms of Universal Statement

∃ x, such that P(x) and Q(x)

Can always be written as

∃ x ∈ D, such that Q(x)

where D is the set of all x for which P(x) is true.

Equivalent forms of Universal Statement

❑ **Example:** Express the proposition: "All human beings are intelligent" in predicate logic.

Let I(x) = x, is intelligent

H(x) = x is human being

Then

$$\forall x, H(x) \rightarrow I(x)$$

Or Equivalently

$$\forall x \in D, \ I(x)$$

Where D is a set of all x for which H(x) is true.

Equivalent forms of Existential Statement

❑ **Example:** Use the predicate logic to express the system specification.

1. Every mail message larger than 1 megabyte will be compressed.
2. If a user is active, at least one network link will be available.

❑ **Solution**:

Let $S(m,y)$ = Mail message larger than Y megabyte

$S(m,1)$ = Mail message larger than 1 megabyte

$C(m)$ = Mail message will be compressed, Then

$$\forall m, S(m, 1) \rightarrow C(m)$$

- Second problem do it yourself.

Negation of a Universal Statement

$\forall x \in D, Q(x)$

Its negation is logically equivalent to

$\exists x \in D, \; A \; Q(x)$

That is

$\sim \left(\forall x \in D, Q(x) \right) \equiv x \in D \; A \sim Q(x)$

$\sim$ (all are) $\equiv$ "Some are not" or "There is at least one that is not"

Nested Quantifiers

- Quantifier within the scope of another quantifier

  $\forall x \, \exists y \, (x + y = 0)$, where the domain of x and y consists of all real numbers.

- For every real number x there is a real number y such that, $x + y = 0$.

  OR

- Every real number has an additive inverse.

❑ Commonly occur in mathematics and computer science.

Nested Quantifiers

❑ **Example:**

• Translate into English the following

$$\forall x, \forall y, \big((x > 0) \text{ A } (y < 0) \rightarrow (xy < 0)\big)$$

where the domain of x and y consists of all real numbers.

Nested Quantification as Loops

❑ It is sometimes easier to think of nested quantification in terms of nested loops.

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

- To see whether it is true.
    - Loop through the values of x
    - For each x, loop through the values of y
    - If P(x , y) is true for all values of x and y, (o) is true.
    - If we ever hit a value x, for which we hit a value y for which P(x , y) is false, (o) is false.

Nested Quantification as Loops

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

- To see whether it is true.
    - Loop through the values of x
    - For each x, loop through the values of y, until we find a y for which P(x , y) is true.
    - If for evert x, we hit such a y, (o) is true
    - If for some x, we never hit such a y, (o) is false.

Nested Quantification as Loops

$$\exists\, x \,,\, \forall\, y \,,\, \mathbf{P(x, y)}$$

$$\exists\, x \,,\, \exists\, y \,,\, P(x, y)$$

"Try it Yourself"

Negating Nested Quantification

❏ Statements involving nested quantifiers can be negated by successively applying rules of negating single quantifier statements.

❏ For Example

- Express the negation of $\forall x, \exists y (xy = 1)$

- $\sim(\forall x, \exists y (xy = 1)) \equiv \exists x \sim \exists y (xy = 1)$
- $\sim(\forall x, \exists y (xy = 1)) \equiv \exists x \, \forall y (xy = 1)$
- $\sim(\forall x, \exists y (xy = 1)) \equiv \exists x \, \forall y (xy \neq 1)$

Arguments with Quantified Statements

❑ Universal modus ponens.

$\forall x$, if P(x) then Q(x)

P(a) for a particular a

$\therefore$ Q(a)

$\forall x \left(p(x) \rightarrow Q(x) \right)$

P(a) for a particular a

$\therefore$ Q(a)

Different Representations of the same concept (argument form)

Arguments with Quantified Statements

❑ **Example**: Is this argument valid? Why?

- If a integer is even, then its square is even k is particular integer that is even

  ∴ k^2 is even

❑ **Solution**: Let E(x) be "an integer is even"

- S(x) be "its square is even", Then

$$\forall x, \text{if } E(x) \text{ then } S(x)$$

$$\underline{E(k) \text{ for a particular k}}$$
$$\therefore S(k)$$

- This argument has the form of "universal modus ponens". Therefore it is a valid argument.

Arguments with Quantified Statements

❑ Universal modus Tollens:

$\forall x$, if P(x) then Q(x)

$\sim$Q(a) for a particular a
$\therefore \sim$P(a)

$\forall x, \forall x \left(p(x) \rightarrow Q(x) \right)$

$\sim$Q(x) for a particular a
$\therefore \sim$P(a)

Arguments with Quantified Statements

❑ **Example**: Recognizing the form of Universal Modus Tollens.

- Rewrite the following argument using quantifiers, variables, and predicate symbols. Write the major premise in conditional form. In this argument valid? why?
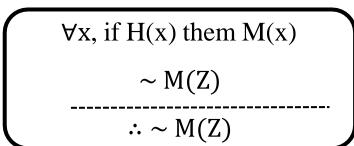
> All Human beings are mortal
>
> Zeus is not mortal.
> --
> ∴ Zeus is not human

❑ **Solution**: The major premise can be rewritten as ∀x, if x is human then x is mortal.

Let H(x) be "x is human", let M(x) be "x is mortal", and let Z stand for Zeus. The argument becomes.

> ∀x, if H(x) them M(x)
>
> ~ M(Z)
> ----------------------------------
> ∴ ~ M(Z)

This argument has the form of universal modus Tollens and is therefore valid.

Proof
for your
understanding.

Proofs

❑ Simply "A Mathematical Proof is a carefully reasoned argument to convince a skeptical listener.

❑ **Importance**:
  • If you have a conjecture, the only way you can safely be sure about its correctness is by presenting a valid proof.

  • While trying to prove something, we may gain a great deal of understanding and knowledge, even if we fail.

Proofs

❏ More formally

- "A mathematical proof of a proposition is a chain of logical deductions leading to the proposition from a bas set of axioms.

❏ Proposition:

❏ Logic:

❏ Axioms:

- Propositions that are simply accepted as true.
- For Example: "There is a straight line segment between every pair of points".

Proofs

❑ **Proving Implications:**

- Many theorems are of the form

  - $P \implies Q$, P implies Q, or If P then Q.

- If $ax^2 + bx + c = 0$ and $a \neq 0$, then

  - $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

- If n is an even integer greater than 2, then n is a sum of two primes.

❑ To prove: Method 1:

- Write , "Assume P"
- Show that Q logically follows

Proofs

❑ **Proving Implications:**

  ❑ Example

For any two positive numbers x and y,

- $\sqrt{xy} \leq \dfrac{x+y}{2}$

Proof: Assume x and y are positive numbers,

- $\left(x - y\right)^2 \left(=\sqrt{0} \quad \sqrt{}\right)$

By algebra this implies

- $x + y - 2\sqrt{x}\sqrt{y} \geq 0$

Moving $2\sqrt{x}\sqrt{y}$ to the other side, we get that.

- $x + y \geq 2\sqrt{x}\sqrt{y}$

Dividing both sides by 2 yields the inequality

- $\dfrac{x+y}{2} \geq \sqrt{xy}$ or $\sqrt{xy} \leq \dfrac{x+y}{2}$

Proofs

❑ **Proving Implications:**

- Method 2: Prove the contrapositive.
  - $\sim P \implies \sim Q$
  - $P \implies Q \equiv \sim P \implies \sim Q$

  Therefore, proving one is as good as proving the other. Proceed as follows,

- Write "We prove the contrapositive." and then state the contrapositive.
- Proceed as in Method #1.

Proofs

Example:

If r is irrational, then $\sqrt{r}$ is also irrational

Proof:

We prove the contrapositive: If $\sqrt{r}$ is rational, then r is rational.

Assume $\sqrt{r}$ is rational. Then there exist integers m and n such that,

$$\sqrt{r} = \frac{m}{n}$$

Squaring both sides

$$r = \frac{m^2}{n^2}$$

Since m^2 and n^2 are integers, so r is rational.

Proofs

❑ **Direct Proof:**

Method 1 is an example of "Direct Proof".

Lets look at some more examples of Direct proof.

Proofs

❑ **Example:** For all integers a and b, if a and b are positive and a divides b, then a ≤ b.

Proof: Assume a and b are positive integers and a divides b.

Then there exists an integer k such that,

$$B = a*k$$

Since both a and b are positive, it follows that

$$1 \leq k$$

Multiplying both sides by a we get

$$a \leq a*k = b$$

$$a \leq b$$

Proofs

❑ **Example:** For all integers a, b, and c, if a divides b and b divides c, then a divides c.

Proof: Assume a, b, and c are integers, such that a divides b, and b divides c.

Then there exist integer r and s, such that,

$$b = a*r \text{ and } c = b*s$$

By substitution

$$c = (a*r)*s$$

$$c = a*(r*s)$$

Let k=r*s , then k is an integer, since it is a product of integers, and therefore

$$c = a*k$$

Thus a divides c.

Proofs

Proof by Division into cases.

- Breaking a proof into cases, and proving each case separately.

- Useful for complicated proofs.

❑ **Example:** Any two consecutive integers have opposite parity.

Proof: Assume m and m+1 be the two consecutive integers. We break the proof in two cases.

Case 1: (m is Even): This means m=2k, for some integer k. Thus

$$m+1 = 2k + 1$$

which is odd, by definition of odd numbers. Hence in this case one of "m" and "m+1" is even and the other is odd.

Proofs

Proof by Division into cases.

Proof: Case 2: (m is Odd): in this case,

$$m = 2k + 1 \text{ , for some integer k}$$

Thus

$$m + 1 = 2k + 1 + 1$$
$$= 2k + 2$$
$$= 2(k+1)$$

But k+1 is integer, as it is a sum of two integers. Thus m+1 is twice some integers, hence m+1 is even.

Hence in this case also one of "m" and "m+1" is even and the other is odd.

Proofs

Proof by Division into cases.

- This is another type of "Direct Proof"
- Lets look at another example.

❑ **Example:** "If a and b are any integers not both zero, and if q and r are any integers such that.

$$a = b*q + r$$

Then

$$gcd(a,b) = gcd (b,r)$$

(gcd= Greatest Common Divisor)

Proofs

Indirect Proofs:

- Proof by contrapositive is an example of indirect proof.

- Another common kind of indirect proof is "proof by contradiction".

- "You show that if a proposition were false, then same false fact would be true."

❑ **Method:**

1. Write, "We use proof by contradiction"
2. Write, "Suppose P is false"
3. Deduce something known to be false (Logical contradiction).
4. Write "This is a contradiction, therefore P must by false."

Proofs

Proof by Contradiction:

- ❑ **Example:** $\sqrt{2}$ is Irrational.

- ❑ **Proof:** We use proof by contradiction. Suppose $\sqrt{2}$ is rational. Then there exist integers m and n with no common factors such that.

$$\sqrt{2} = \frac{m}{n}$$

Squaring both sides gives

$$2 = \frac{m^2}{n^2} \Rightarrow m^2 = 2n^2$$

This means that m^2 is even, which implies that m is even. That is for some integer k.

$$m = 2k$$
$$m^2 = (2k)^2 = 4k^2 = 2n^2$$

Or equivalently

$$n^2 = 2k^2$$

Consequently n^2 is even, and so n is even.

Hence both "m" and "n" have a common factor of 2, which contradicts our supposition. Hence the supposition is false, and the theorem is true.

Proofs

Proof by Contradiction:

❑ **Example:** $\sqrt{2}$ is Irrational using Geometry.

❑ **Proof:** Uses the idea of Commensurability. (Ch:1, P:8-10)

Proofs

Proof by Contradiction:

Example:

- ❑ **Theorem:** "The Quadrature of a circle is impossible".

- ❑ **Proof:** Uses the concept of Algebraic numbers, Constructible numbers, and transcendental numbers. (Ch:1, P:25)

Proofs

Proof by Contradiction:

Example

- ❑ **Theorem:** **"**If a straight line falling on two straight lines makes the alternate angles equal to one another, the straight lines will be parallel".

- ❑ **Proof:** Ch:2, P:44.

Proofs

Summary:

- ❑ **Direct Proof**

- ❑ **Disproof by Counter example**

- ❑ **Proof by Contradiction**

- ❑ **Proof by Contrapositive**