SCSI1013: Discrete Structures

CHAPTER 1

Quantifiers & Proof Technique

QUANTIFIERS

- Most of the statements in mathematics and computer science are not described properly by the propositions.
- Since most of the statements in mathematics and computer science use **variables**, the system of logic must be extended to include **statements with the variables**.

QUANTIFIERS (cont.)

- Let $P(x)$ is a statement with variable x and A is a set.
- P a **propositional function** or also known as **predicate** if for each x in A, $P(x)$ is a proposition.
- Set A is the **domain of discourse** of P.
- Domain of discourse -> the particular domain of the variable in a propositional function.

QUANTIFIERS (cont.)

- A **predicate** is a statement that contains variables.

- **Example:**

  $P(x) : x > 3$

  $Q(x,y) : x = y + 3$

  $R(x,y,z) : x + y = z$

Example

- $x^2 + 4x$ is an odd integer

  (domain of discourse is set of positive numbers).
- $x^2 - x - 6 = 0$

  (domain of discourse is set of real numbers).
- UTM is rated as Research University in Malaysia

  (domain of discourse is set of research university in Malaysia).

QUANTIFIERS (cont.)

- A predicate becomes a proposition if the variable(s) contained is(are)
  - **Assigned specific value(s)**
  - **Quantified**

Example

- $P(x) : x > 3$.

  What are the truth values of $P(4)$- (true) and $P(2)$(false)?
- $Q(x,y) : x = y + 3$.

  What are the truth values of $Q(1,2)$ and $Q(3,0)$?

Propositional functions 2

- Let P(x) = "x is a multiple of 5"
  - For what values of x is P(x) true?
- Let P(x) = x+1 > x
  - For what values of x is P(x) true?
- Let P(x) = x + 3
  - For what values of x is P(x) true?

QUANTIFIERS (cont.)

- Two types of quantifiers:
  - **Universal**
  - **Existential**

QUANTIFIERS (cont.)

- Let *A* be a propositional function with domain of discourse *B*. The statement

  for every x, $A(x)$

  is **universally quantified statement**
- Symbol ∀ called a **universal quantifier** is used "**for every**".
- Can be read as "**for all**", "**for any**".

Universal quantifiers 1

- Represented by an upside-down A: ∀
  - It means "for all"
  - Let P(x) = x+1 > x
- We can state the following:
  - ∀x P(x)
  - English translation: "for all values of x, P(x) is true"
  - English translation: "for all values of x, x+1>x is true"

QUANTIFIERS (cont.)

- The statement can be written as

$$\forall x\ A(x)$$

- Above statement is true if $A(x)$ is true for every x in *B* (false if $A(x)$ is false for at least one x in *B*).
  OR In order to prove that a universal quantification is true, it must be shown for ALL cases
  In order to prove that a universal quantification is false, it must be shown to be false for only ONE case
- A value x in the domain of discourse that makes the statement $A(x)$ *false* is called a **counterexample** to the statement.

Example

- Let the universally quantified statement is

$$\forall x\ (x^2 \geq 0)$$

- Domain of discourse is the set of real numbers.
- **This statement is true** because for every real number x, it is true that the square of x is positive or zero.

Example

- Let the universally quantified statement is

$$\forall x\ (x^2 \leq 9)$$

- Domain of discourse is a set B = {1, 2, 3, 4}
- When x = 4, the statement produce false value.
- Thus, **the above statement is false** and the counterexample is 4.

innovative • entrepreneurial • global www.utm.my

QUANTIFIERS (cont.)

- Easy to prove a universally quantified statement is true or false if the domain of discourse is not too large.
- What happen if the domain of discourse contains a large number of elements?
- For example, a set of integer from 1 to 100, the set of positive integers, the set of real numbers or a set of students in Faculty of Computing. It will be hard to show that every element in the set is *true*.

Use existential quantifier!!

innovative • entrepreneurial • global www.utm.my

QUANTIFIERS (cont.)

- Let *A* be a propositional function with domain of discourse *B*. The statement

There exist x, $A(x)$

is **existentially quantified statement**

- Symbol ∃ called an **existential quantifier** is used "**there exist**".
- Can be read as "**for some**", "**for at least one**".

innovative • entrepreneurial • global www.utm.my

QUANTIFIERS (cont.)

- The statement can be written as

$$\exists x\ A(x)$$

- Above statement is true if $A(x)$ is true for at least one x in *B* (false if every x in *B* makes the statement $A(x)$ false).

- **Just find one x that makes $A(x)$ true!**

innovative • entrepreneurial • global www.utm.my

Example

- Let the existentially quantified statement is

$$\exists x \left(\frac{x}{x^2+1} = \frac{2}{5} \right)$$

- Domain of discourse is the set of real numbers.
- **Statement is true** because it is possible to find at least one real number x to make the proposition true.

innovative • entrepreneurial • global www.utm.my

- For example, if x = 2, we obtain the true proposition as below

$$\left(\frac{x}{x^2+1} = \frac{2}{5} \right) = \left(\frac{2}{2^2+1} = \frac{2}{5} \right)$$

innovative • entrepreneurial • global www.utm.my

Negation of Quantifiers

- Distributing a negation operator across a quantifier changes a universal to an existential and vice versa.

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

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

Example

- Let $P(x)$ = x is taking Discrete Structure course with the domain of discourse is the set of all students.
  - $\forall x\ P(x)$: All students are taking Discrete Structure course.
  - $\exists x\ P(x)$: There is some students who are taking Discrete Structure course.

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

$\neg\exists x\ P(x)$: None of the students are taking Discrete Structure course.

$\forall x \neg P(x)$: All students are not taking Discrete Structure course.

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

$\neg\forall x\ P(x)$: Not all students are taking Discrete Structure course.

$\exists x \neg P(x)$: There is some students who are not taking Discrete Structure course

Translating from English

- Consider "For every student in this class, that student has studied calculus"
- Rephrased: "For every student x in this class, x has studied calculus"
  - Let C(x) be "x has studied calculus"
  - Let S(x) be "x is a student"
- $\forall$x C(x)
  - True if the universe of discourse is all students in this class

Translating from English 2

- What about if the unvierse of discourse is all students (or all people?)
  - $\forall x\ (S(x) \wedge C(x))$
    - This is wrong! Why? (because this statement says that all people are students in this and have studied calculus)
  - $\forall x\ (S(x) \rightarrow C(x))$

Translating from English 3

- Consider:
  - "Some students have visited Mexico"
  - "Every student in this class has visited Canada or Mexico"
- Let:
  - S(x) be "x is a student in this class"
  - M(x) be "x has visited Mexico"
  - C(x) be "x has visited Canada"

Translating from English 4

- Consider: "Some students have visited Mexico"
  - Rephrasing: "There exists a student who has visited Mexico"

    $\exists x\, M(x)$
  - True if the universe of discourse is all students
- What about if the universe of discourse is all people?

  $\exists x\, (S(x) \wedge M(x))$
  - $\exists x\, (S(x) \rightarrow M(x))$
    - This is wrong! Why?

    suppose someone not in the class = F->T or F->F, both make the statement true

Translating from English 5

- Consider: "Every student in this class has visited Canada or Mexico"
- $\forall x\, (M(x) \vee C(x))$
  - When the universe of discourse is all students
- $\forall x\, (S(x) \rightarrow (M(x) \vee C(x)))$
  - When the universe of discourse is all people

Proof Techniques

- **Mathematical systems consists:**
  - Axioms: assumed to be true.
  - Definitions: used to create new concepts.
  - Undefined terms: some terms that are not explicitly defined.
  - Theorem

Proof Techniques

- **Theorem**
  - Statement that can be shown to be true (under certain conditions)
  - Typically stated in one of three ways:
    - As Facts
    - As Implications
    - As Bi-implications

Proof Techniques (cont.)

Direct Proof (Direct Method)

- Proof of those theorems that can be expressed in the form $\forall x\, (P(x) \rightarrow Q(x))$, D is the domain of discourse.
- Select a particular, but arbitrarily chosen, member a of the domain D.
- Show that the statement $P(a) \rightarrow Q(a)$ is true. (Assume that $P(a)$ is true).
- Show that $Q(a)$ is true.
- By the rule of Universal Generalization (UG), $\forall x\, (P(x) \rightarrow Q(x))$ is true.

Example

For all integer x, if x is odd, then x^2 is odd

Or $P(x)$ = is an odd integer

$Q(x) = x^2$ is an odd integer

$$\forall x(P(x) \to Q(x))$$

the domain of discourse is set Z of all integer.

Can verify the theorem for certain value of x.

x=3, x^2 =9 ; odd

Example

- Or show that the square of an odd number is an odd number
- Rephrased: if n is odd, the n^2 is odd

Example (cont.)

- a is an odd integer

$\Rightarrow a = 2n + 1$ → for some integer **n**

$\Rightarrow a^2 = (2n+1)^2$

$\Rightarrow a^2 = 4n^2 + 4n + 1$

$\Rightarrow a^2 = 2(2n^2 + 2n) + 1$

$\Rightarrow a^2 = 2m + 1$ → where $m = 2n^2 + 2n$ is an integer

$\Rightarrow a^2$ → is an odd integer

Proof Techniques (cont.)

- **Indirect Proof**
  - The implication $p \to q$ is **equivalent** to the implication **($\neg q \to \neg p$) (contrapositive)**
  - Therefore, in order to show that $p \to q$ is true, one can also **show that the implication ($\neg q \to \neg p$) is true**.
  - To show that ($\neg q \to \neg p$) is true, assume that the negation of q is true and prove that the negation of p is true.

Example

$P(n)$: n^2+3 is an odd number

$Q(n)$: n is even number

$$\forall n(P(n) \to Q(n))$$

$$P(n) \to Q(n) \equiv \neg Q(n) \to \neg P(n)$$

- $\neg Q(n)$ is true , n is not even (n is odd), so $n=2k+1$

$$n^2 + 3 = (2k+1)^2 + 3$$
$$= 4k^2 + 4k + 1 + 3$$
$$= 4k^2 + 4k + 4$$
$$= 2(2k^2 + 2k + 2)$$

Example (cont.)

$$n^2 + 3 = (2k+1)^2 + 3$$
$$= 4k^2 + 4k + 1 + 3$$
$$= 4k^2 + 4k + 4$$
$$= 2(2k^2 + 2k + 2)$$

$t = 2k^2 + 2k + 2$ → *t is integer*

$n^2 + 3 = 2t$

n^2+3 is an even integer, thus $\neg P(n)$ is true

Which to use

- When do you use a direct proof versus an indirect proof?
- If it's not clear from the problem, try direct first, then indirect second
  - If indirect fails, try the other proofs

Example of which to use

Prove that if n is an integer and n^3+5 is odd, then *n* is even

- Via direct proof
  - $n^3+5 = 2k+1$ for some integer *k* (definition of odd numbers)
  - $n^3 = 2k+6$
  - $n = \sqrt[3]{2k+6}$
  - Umm…
- So direct proof didn't work out. Next up: indirect proof

Example of which to use

- Prove that if n is an integer and n^3+5 is odd, then *n* is even

- Via indirect proof
  - Contrapositive: If *n* is odd, then n^3+5 is even
  - Assume *n* is odd, and show that n^3+5 is even
  - n=2k+1 for some integer k (definition of odd numbers)
  - $n^3+5 = (2k+1)^3+5 = 8k^3+12k^2+6k+6 = 2(4k^3+6k^2+3k+3)$
  - As $2(4k^3+6k^2+3k+3)$ is 2 times an integer, it is even

Proof Techniques (cont.)

Proof by Contradiction

Assume that the hypothesis is true and that the conclusion is false and then, arrive at a contradiction.

Proposition if *P* then *Q*
Proof. Suppose *P* and ~*Q*

Since we have a contradiction, it must be that Q is true

Example

Prove that there are infinitely many prime numbers.
Proof:
▪Assume there are not infinitely many prime numbers, therefore they are can be listed, i.e. $p_1, p_2, \ldots, p_n$
▪Consider the number $q = p_1 \times p_2 \times \ldots \times p_n + 1$.
▪ *q* is either prime or not divisible, but not listed above. Therefore, *q* is a prime. However, it was not listed.
▪**Contradiction**! Therefore, there are infinitely many primes numbers.

Example

- For all real numbers x and y, if $x+y \geq 2$, then either $x \geq 1$ or $y \geq 1$.

Proof
- Suppose that the conclusion is false. Then
  $x < 1$ and $y < 1$
  Add these inequalities, $x+y < 1+1 = 2$ (**$x+y < 2$**)
- **Contradiction**
- Thus we conclude that the statement is true.

Example

Suppose $a \in Z$. If a^2 is even, then *a* is even

Proof

- Contradiction: Suppose a^2 is even and *a* is not even.
- Then a^2 is even, and *a* is odd
- So $a = 2c + 1$, then $a^2 = (2c+1)^2 = 4c^2 + 4c + 1 = 2(2c^2 + 2c) + 1$
- Thus a^2 is even and a^2 is not even, a contradiction
- The original supposition that is a^2 even and *a* is odd could not be true