
CS 2305: Discrete Mathematics for Computing I

Lecture 10

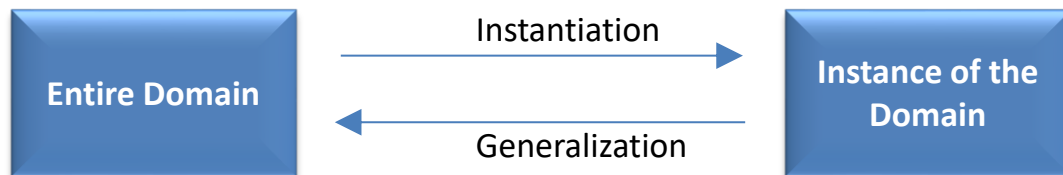
- KP Bhat

Additional Rules of Inference for Quantified Statements (Recap)

Mnemonics

x: Unspecified member of the domain

c: Specific member of the domain



| TABLE 2 Rules of Inference for Quantified Statements. | |
|--|----------------------------|
| Rule of Inference | Name |
| $\frac{\forall x P(x)}{\therefore P(c)}$ | Universal instantiation |
| $\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$ | Universal generalization |
| $\frac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$ | Existential instantiation |
| $\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$ | Existential generalization |

Universal Instantiation (UI)

$$\frac{\forall xP(x)}{\therefore P(c)}$$

Example:

Our domain consists of all dogs and Fido is a dog.

P: “All dogs are cuddly.”

C: “Therefore, Fido is cuddly.”

Universal Generalization (UG)

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

P: Predicate is true for any arbitrarily selected member of the domain of discourse

C: \therefore Predicate is universally true over the domain of discourse

By arbitrary we mean it is not any specific element of the domain and we cannot make any other assumption about c other than it comes from the domain.

UG is used often implicitly in Mathematical Proofs.

Existential Instantiation (EI)

$$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$$

Example:

P: “There is someone who got an A in the course.”

[Upon verification we find that the student who got an A is named Michelle]

C: “Michelle got an A in the course”

Note that we are not selecting an arbitrary element from the domain. Rather we are selecting a specific element from the domain for which $P(c)$ is true

Existential Generalization (EG)

$$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$$

Example:

P: “Michelle got an A in the class.”

C: “Therefore, someone got an A in the class.”

Again we are not selecting an arbitrary element from the domain.

Using Rules of Inference₁

Example 1: Using the rules of inference, construct a valid argument to show that
“John Smith has two legs”

is a consequence of the premises:

“Every man has two legs.” “John Smith is a man.”

Solution: Let $M(x)$ denote “ x is a man” and $L(x)$ “ x has two legs” and let John Smith be a member of the domain.

Valid Argument:

| Step | Reason |
|---------------------------------------|--------------------------------|
| 1. $\forall x(M(x) \rightarrow L(x))$ | Premise |
| 2. $M(J) \rightarrow L(J)$ | UI from (1) |
| 3. $M(J)$ | Premise |
| 4. $L(J)$ | Modus Ponens using (2) and (3) |

$$\frac{\forall x P(x)}{\therefore P(c)}$$
$$\frac{p \quad p \rightarrow q}{\therefore q}$$

Using Rules of Inference₂

Example 2: Use the rules of inference to construct a valid argument showing that the conclusion
“Someone who passed the first exam has not read the book.”

follows from the premises

“A student in this class has not read the book.”

“Everyone in this class passed the first exam.”

Solution: Let $C(x)$ denote “ x is in this class,” $B(x)$ denote “ x has read the book,” and $P(x)$ denote “ x passed the first exam.”

First we translate the
premises and conclusion
into symbolic form.

$$\frac{\begin{array}{l} \exists x(C(x) \wedge \neg B(x)) \\ \forall x(C(x) \rightarrow P(x)) \end{array}}{\therefore \exists x(P(x) \wedge \neg B(x))}$$

Continued on next slide →

Using Rules of Inference₃

Valid Argument:

| Step | Reason |
|---------------------------------------|-------------------------|
| 1. $\exists x(C(x) \wedge \neg B(x))$ | Premise |
| 2. $C(a) \wedge \neg B(a)$ | EI from (1) |
| 3. $C(a)$ | Simplification from (2) |
| 4. $\forall x(C(x) \rightarrow P(x))$ | Premise |
| 5. $C(a) \rightarrow P(a)$ | UI from (4) |
| 6. $P(a)$ | MP from (3) and (5) |
| 7. $\neg B(a)$ | Simplification from (2) |
| 8. $P(a) \wedge \neg B(a)$ | Conj from (6) and (7) |
| 9. $\exists x(P(x) \wedge \neg B(x))$ | EG from (8) |

$$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$$

$$\frac{p \wedge q}{\therefore p}$$

$$\frac{\forall x P(x)}{\therefore P(c)}$$

$$\frac{p \quad p \rightarrow q}{\therefore q}$$

$$\frac{p \wedge q}{\therefore p}$$

$$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$$

$$\frac{p \quad q}{\therefore p \wedge q}$$

Returning to the Socrates Example

$$\forall x (Man(x) \rightarrow Mortal(x))$$

$$Man(Socrates)$$

$$\therefore Mortal(Socrates)$$

Valid Argument

Step

1. $\forall x (Man(x) \rightarrow Mortal(x))$

2. $Man(Socrates) \rightarrow Mortal(Socrates)$

3. $Man(Socrates)$

4. $Mortal(Socrates)$

Reason

Premise

UI from (1)

Premise

MP from (2) and (3)

$$\frac{\forall x P(x)}{\therefore P(c)}$$

$$\frac{p \quad p \rightarrow q}{\therefore q}$$

Universal Modus Ponens

Universal Modus Ponens combines universal instantiation and modus ponens into one rule.

$$\frac{p \quad p \rightarrow q}{\therefore q}$$

$$\frac{\forall x P(x)}{\therefore P(c)}$$

$$\frac{\forall x(P(x) \rightarrow Q(x)) \quad P(a), \text{ where } a \text{ is a particular element in the domain}}{\therefore Q(a)}$$

Universal Modus Ponens is used in many mathematical arguments

Universal Modus Tollens

Similarly Universal Modus Tollens combines universal instantiation and modus tollens into one rule.

$$\frac{\neg q \quad p \rightarrow q}{\therefore \neg p}$$

$$\frac{\forall x P(x)}{\therefore P(c)}$$

$$\frac{\forall x (P(x) \rightarrow Q(x)) \quad \neg Q(a), \text{ where } a \text{ is a particular element in the domain}}{\therefore \neg P(a)}$$

Introduction to Proofs

Proofs of Mathematical Statements

A *proof* is a valid argument that establishes the truth of a statement.

In math, CS, and other disciplines, informal proofs which are generally shorter, are generally used.

- More than one rule of inference are often used in a step.
- Steps may be skipped.
- The rules of inference used are not explicitly stated.
- Easier for to understand and to explain to people.
- But it is also easier to introduce errors.

Proofs have many practical applications:

- verification that computer programs are correct
- establishing that operating systems are secure
- enabling programs to make inferences in artificial intelligence
- showing that system specifications are consistent

Definitions (1)

A **theorem** is a statement that can be shown to be true using:

- definitions
- other theorems
- axioms (statements which are given as true, also known as postulates)
- rules of inference

Axioms of Euclidean Plane Geometry

1. A straight line may be drawn between any two points
2. Any terminated straight line may be extended indefinitely
3. A circle may be drawn with any given point as center and any given radius
4. All right angles are equal
5. For any given point not on a given line, there is exactly one line through the point that does not meet the given line

Definitions (2)

A **lemma** is a ‘helping theorem’ or a result which is needed to prove a theorem.

- Complicated proofs are usually easier to understand when they are proved using a series of lemmas

A **corollary** is a result which follows directly from a theorem.

Less important theorems are sometimes called **propositions**.

A **conjecture** is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a theorem. It may turn out to be false.

- For example Millennium Problems from the Clay Mathematics Institute <https://www.claymath.org/millennium-problems>

A Commonly Used Proof Technique

Many theorems have the form:

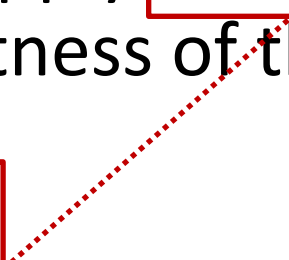
$$\forall x(P(x) \rightarrow Q(x))$$

The first step is to show that

$$P(c) \rightarrow Q(c)$$

is true for c , some arbitrary element of the domain

The next step is to apply universal generalization to establish the correctness of the theorem.


$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

Direct Proof

- A direct proof shows that a conditional statement $p \rightarrow q$ is true by showing that if p is true, then q must also be true
- We assume that p is true and use axioms, definitions, and previously proven theorems, together with rules of inference, to show that q must also be true.

Background Information: Even and Odd Integers

Definition: The integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k , such that $n = 2k + 1$. Note that every integer is either even or odd and no integer is both even and odd

Direct Proof: $p \rightarrow q$ (1)

Example: Give a direct proof of the theorem “If n is an odd integer, then n^2 is odd.”

Solution:

Let us take an arbitrary odd number n .

Then $n = 2k + 1$, for some integer k

Squaring both sides of the equation, we get:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2r + 1,$$

where $r = 2k^2 + 2k = 2(k^2 + k)$, an even integer.

Since r is even, $2r + 1$ is odd, $\therefore n^2$ is odd

We have proved directly that if n is an odd integer, then n^2 is an odd integer.

(marks the end of the proof. Sometimes **QED** is used instead.)

Direct Proof: $p \rightarrow q$ (2)

Example: Give a direct proof of the theorem “If m and n are both square numbers, then mn is also a square number.”

Solution:

Let us take arbitrary square numbers m and n .

By definition there exist numbers s and t such that

$$m = s^2$$

$$n = t^2$$

$$m * n = s^2 * t^2 = (st)^2, \text{ which is also a square number}$$

We have proved directly that if m and n are both square numbers, then mn is also a square number.

QED

Background Information: Rational Numbers

Definition: The real number r is *rational* if there exist integers p and q where $q \neq 0$ such that $r = p/q$

Direct Proof: $p \rightarrow q$ (3)

Example: Prove that the sum of two rational numbers is rational.

Solution:

Let us take arbitrary rational numbers r and s

By definition there must be integers p, q and also t, u such that

$$r = p / q, \quad s = t / u, \quad u \neq 0, \quad q \neq 0$$

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{qu} = \frac{v}{w} \quad \begin{array}{l} \text{where } v = pu + qt \\ w = qu \neq 0 \end{array}$$

We have proved directly that the sum of two rational numbers is rational.

QED