CMSC 250

Discrete Structures

Rules of Inference for Quantified Statements and Proofs

Universal Instantiation

Definition

We conclude that $P(c)$ is true, where c is a particular member of the domain, given the premise $\forall x P(x)$

Example

$$\frac{\text{All Martians are green}}{\therefore \text{ Marvin is green}}$$

given, Marvin ϵ Martians.

Universal Instantiation

$$\frac{\forall x \epsilon D[P(x)]}{\therefore P(c), \text{ for any } c \epsilon D}$$

Universal Generalization

Definition

$\forall x P(x)$ is true, given the premise that $P(c)$ is true for all elements c in the domain.
The element c must be an arbitrary, and not a specific element of the domain.

Universal Generalization

$$\frac{P(c), \text{ for some } c \epsilon D \text{ (selected arbitrarily)}}{\therefore \forall x \epsilon D[P(x)]}$$

Example

$$\frac{\begin{array}{l} P(c) : c \geq 0 \\ c \epsilon \mathbb{N}[P(c)] \end{array}}{\therefore \forall x \epsilon \mathbb{N}[P(x)]}$$

Existential Instantiation

Definition

If we know $\exists x P(x)$ is true, we can conclude there is an element c in the domain for which $P(c)$ is true.

existential instantiation

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

If you know something exists, you can give it a name.

Existential Generalization

Definition

For a particular element c, if we know $P(c)$ is true, we can conclude that $\exists x P(x)$ is true.

Existential Generalization

$$\frac{P(c) \text{ for some } c \,\epsilon\, \text{D}}{\therefore \exists x \epsilon D[P(x)]}$$

Summary for the rules of inference

Definition

Universal Instantiation	$\begin{array}{l} \quad\underline{(\forall x)[P(x)]} \\ \therefore P(c) \end{array}$
Universal Generalization	$\begin{array}{l} \quad\underline{P(c) \text{ for arbitrary element } c} \\ \therefore (\forall x)[P(x)] \end{array}$
Existential Instantiation	$\begin{array}{l} \quad\underline{(\exists x)[P(x)]} \\ \therefore P(c) \text{ for some element } c \end{array}$
Existential Generalization	$\begin{array}{l} \quad\underline{P(c) \text{ for some element } c} \\ \therefore (\exists x)[P(x)] \end{array}$

Methods of Proofs

Terminology

Definition

A *Theorem* is a statement that can be shown to be true.
A *Lemma* is a less important theorem that is helpful in the proof of other results.
A *Corollary* is a theorem that can be established directly from a theorem that has been proved.
A *Conjecture* is a statement that is being proposed to be a true statement.
A *Proof* is a valid argument that establishes the truth of a theorem.
An *Axiom* is a statement we assume to be true.

What is a proof?

A good proof should have:

- A clear statement of what is to be proved (labeled as Theorem, Lemma, Proposition, or Corollary).
- The word "Proof" to indicate where the proof starts.
- A clear indication of flow.
- A clear justification for each step.
- A clear indication of the conclusion.
- The abbreviation "QED" ("Quod Erat Demonstradum" or "that which was to be proved") or equivalent to indicate the end of the proof.

Summary of Proof Methods

- Direct proof
- Proof by contraposition.
- Proof by contradiction.
- Exhaustive Proof.
- Proof by cases.

Statement of Theorems

The following are equivalent:

- The sum of two positive integers is positive.
- If m, n are positive integers then their sum m + n is a positive integer.
- For all positive integers m, n their sum m + n is a positive integer.
- $(\forall m, n \epsilon \mathbb{Z})[((m > 0) \wedge (n > 0)) \rightarrow ((m + n) > 0)]$

Number Definitions

Definition

An integer n is *even* if $n = 2k$ or some integer k, and is *odd* if $n = 2k + 1$ for some integer k.

Rational

A number q is *rational* if there exist integers a, b with $b \neq 0$ such that $q = \frac{a}{b}$.

Irrational

A real number that is not rational is *irrational*.

Closure

- $\mathbb{Z}$ is closed under addition

  If a,$b \in \mathbb{Z}$ then $a + b \in \mathbb{Z}$

- $\mathbb{Q}^{\neq 0}$ is closed under division.

  If q, $r \in \mathbb{Q}^{\neq 0}$ then $\frac{q}{r} \in \mathbb{Q}^{\neq 0}$

- $\mathbb{Z}^{\neq 0}$ is not closed under division.

  $\frac{3}{5} \notin \mathbb{Z}^{\neq 0}$

Direct Proofs

- The square of an even number is even.
- The product of two odd numbers is odd.
- The sum of two rational numbers is rational.

Proof by Contraposition

- If $3n + 2$ is odd, where n is an integer, then n is odd.