Logic & Proofs (Lecture – 5)

Dr. Nirnay Ghosh

Rules of Inference for Quantified Statements

- **Universal instantiation** is the rule of inference used to conclude that $P(c)$ is true, where c is a particular member of the domain, given the premise $\forall x P(x)$.
  - Example: Universal instantiation is used when we conclude from the statement "All women are wise" that "Lisa is wise," where Lisa is a member of the domain of all women.
- **Universal generalization** is the rule of inference that states that $\forall x P(x)$ is true, given the premise that $P(c)$ is true for all elements c in the domain.
  - This is used when we show that $\forall x P(x)$ is true by taking an arbitrary element c from the domain and show that $P(c)$ is true. The element c that we select must be an arbitrary, and not a specific, element of the domain.

Rules of Inference for Quantified Statements

- **Existential instantiation** is the rule that allows us to conclude that there is an element c in the domain for which $P(c)$ is true if we know that $\exists x P(x)$ is true.
  - We cannot select an arbitrary value of c here, but rather it must be a c for which $P(c)$ is true. Usually we have no knowledge of what c is, only that it exists. Because it exists, we may give it a name (c) and continue our argument
- **Existential generalization** is the rule of inference that is used to conclude that $\exists x P(x)$ is true when a particular element c with $P(c)$ true is known. That is, if we know one element c in the domain for which $P(c)$ is true, then we know that $\exists x P(x)$ is true.

Rules of Inference for Quantified Statements

TABLE 2 Rules of Inference for Quantified Statements.

Rule of Inference	*Name*
$\forall x\, P(x)$ $\therefore\ P(c)$	Universal instantiation
$P(c)$ for an arbitrary c $\therefore\ \forall x\, P(x)$	Universal generalization
$\exists x\, P(x)$ $\therefore\ P(c)$ for some element c	Existential instantiation
$P(c)$ for some element c $\therefore\ \exists x\, P(x)$	Existential generalization

Introduction to Proofs

- A proof is a valid argument that establishes the truth of a mathematical statement.
- The methods of proof are important not only for proving mathematics statements but also used in many computer science applications.
  - Verifying the correctness of computer programs, establishing that operating systems are secure, making inferences in artificial intelligence, showing that system specifications are consistent, and so on.
- Consequently, understanding the techniques used in proofs is essential both in mathematics and in computer science.

Terminologies

- **Theorem:** It is a statement that can be shown to be true.
  - Example: It may be universal quantification of a conditional statement with one or more premises and a conclusion or some other type of logical statements.
- **Proof:** A proof is a valid argument that establishes the truth of a theorem.
  - The statements used in a proof can include **axioms** (or postulates), which are statements we assume to be true, the premises, if any, of the theorem, and previously proven theorems.
  - Rules of inference, together with definitions of terms, are used to draw conclusions from other assertions, tying together the steps of a proof. In practice, the final step of a proof is usually just the conclusion of the theorem.

Terminologies

- **Lemma:** A less important theorem that is helpful in proving other results.
- **Corollary:** It is a theorem that can be established directly from a theorem that has been proved.
- **Conjecture**: It is statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert.
  - When a proof of a conjecture is found, the conjecture becomes a theorem. Many times conjectures are shown to be false, so they are not theorems.