Math 1019
Discrete Mathematics for Computer Science
Lecture 7
Fall 2021

Saeed Ghasemi

York University

Rules of Inference for Quantified Statements

Definition

- 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 $\forall x P(x)$.
- 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.
- Existential instantiation is the rule of inference 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.
- 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.

Example

Show that the premises "A student in this class has not read the book," and "Everyone in this class passed the first exam" imply the conclusion "Someone who passed the first exam has not read the book."

Solution

Let $C(x)$ be "x is in this class," $B(x)$ be "x has read the book," and $P(x)$ be "x passed the first exam." The premises are $\exists x(C(x) \wedge \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$. The conclusion is $\exists x(P(x) \wedge \neg B(x))$. These steps can be used to establish the conclusion from the premises.

Solution (continued)

(1) $\exists x(C(x) \wedge \neg B(x))$	*Premise*
(2) $C(a) \wedge \neg B(a)$	*Existential instantiation from (1)*
(3) $C(a)$	*Simplification from (2)*
(4) $\forall x(C(x) \rightarrow P(x))$	*Premise*
(5) $C(a) \rightarrow P(a)$	*Universal instantiation from (4)*
(6) $P(a)$	*Modus ponens from (3) and (5)*
(7) $\neg B(a)$	*Simplification from (2)*
(8) $P(a) \wedge \neg B(a)$	*Conjunction from (6) and (7)*
(9) $\exists x(P(x) \wedge \neg B(x))$	*Existential generalization from (8)*

Combining Rules of Inference for Propositions and Quantified Statements

Because universal instantiation and modus ponens are used so often together, this combination of rules is sometimes called universal modus ponens. This rule tells us that if $\forall x(P(x) \rightarrow Q(x))$ is true, and if $P(a)$ is true for a particular element a in the domain of the universal quantifier, then $Q(a)$ must also be true.

Universal modus ponens

$$\frac{\begin{array}{l}\forall x(P(x) \rightarrow Q(x)), \\ P(a), \text{ where a is a particular element in the domain}\end{array}}{Q(a)}$$

Example

Assume that "For all positive integers n, if n is greater than 4, then n^2 is less than 2^n" is true. Use universal modus ponens to show that $100^2 < 2^{100}$.

Solution

Let $P(n)$ denote "$n > 4$" and $Q(n)$ denote "$n^2 < 2^n$." The statement "For all positive integers n, if n is greater than 4, then n^2 is less than 2^n" can be represented by $\forall n(P(n) \rightarrow Q(n))$, where the domain consists of all positive integers. We are assuming that $\forall n(P(n) \rightarrow Q(n))$ is true. Note that $P(100)$ is true because $100 > 4$. It follows by universal modus ponens that $Q(100)$ is true, namely that $100^2 < 2^{100}$.

Universal modus tollens combines universal instantiation and modus tollens and can be expressed in the following way:

Universal modus tollens

$$\frac{\begin{array}{l}\forall x(P(x) \rightarrow Q(x)), \\ \neg Q(a), \text{ where a is a particular element in the domain}\end{array}}{\neg P(a)}$$

1.7. Introduction to Proofs

- In this section we introduce the notion of a proof and describe methods for constructing proofs. A "proof" is a valid argument that establishes the truth of a mathematical statement.
- In practice, most of the proofs in mathematics (outside logic) are informal proofs, where more than one rule of inference may be used in each step, where steps may be skipped, where the axioms being assumed and the rules of inference used are not explicitly stated.
- In this section, and in Section 1.8, we will develop a large arsenal of proof techniques that can be used to prove a wide variety of theorems.

Some Terminology

- Formally, a theorem is a statement that can be shown to be true. The term "theorem" is usually reserved for a statement that is considered at least somewhat important. Less important theorems sometimes are called propositions.
- 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) and previously proven theorems.

Some Terminology

- A less important theorem that is helpful in the proof of other results is called a lemma.
- 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 theorem, usually on the basis of some partial evidence, 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.

Methods of Proving Theorems

- Many theorems in mathematics are of the form $\forall x(P(x) \rightarrow Q(x))$.
- To prove a theorem of the form $\forall x(P(x) \rightarrow Q(x))$, our goal is to show that $P(c) \rightarrow Q(c)$ is true, where c is an arbitrary element of the domain, and then apply universal generalization.
- Recall that $p \rightarrow q$ is true unless p is true but q is false. Thus to prove the statement $p \rightarrow q$, we only need to show that q is true if p is true.

Direct Proofs

A direct proof of a conditional statement $p \rightarrow q$ is constructed when the first step is the assumption that p is true; subsequent steps are constructed using rules of inference, with the final step showing that q must also be true.
Before we show examples of direct proofs we recall the following definition.

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.) Two integers have the same parity when both are even or both are odd; they have opposite parity when one is even and the other is odd.

Example

Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd."

Solution

Note that this theorem states $\forall n(P(n) \rightarrow Q(n))$, where $P(n)$ is "n is an odd integer" and $Q(n)$ is "n^2 is odd." We will show that $P(n)$ implies $Q(n)$ for any (arbitrary) n. In informal proofs like this one (which are common in mathematics) we don't need to explicitly mention the use of universal generalization. To begin a direct proof, assume that the hypothesis of this conditional statement is true, namely, assume that n is odd. By the definition of an odd integer, it follows that $n = 2k + 1$, for some integer k. We want to show that n^2 is also odd. We can square both sides of the equation $n = 2k + 1$. Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. By the definition of an odd integer, we can conclude that n^2 is an odd integer (it is one more than twice an integer).

Example

An integer a is a perfect square if there is an integer b such that $a = b^2$.
Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square.

Solution

To produce a direct proof, we assume that the hypothesis of this conditional statement is true, namely, we assume that m and n are both perfect squares. By the definition of a perfect square, there are integers s and t such that $m = s^2$ and $n = t^2$. The goal of the proof is to show that mn is a perfect square. By substituting s^2 for m and t^2 for n into mn we have $mn = s^2t^2$. Hence, $mn = s^2t^2 = (st)^2$. By the definition of perfect square, it follows that mn is also a perfect square, because it is the square of st, which is an integer.

Proof by Contraposition

Sometimes it is much easier to prove theorems of the form $\forall x(P(x) \rightarrow Q(x))$ using indirect proofs, that do not start with the premises and end with the conclusion.
An very useful type of indirect proof is known as proof by contraposition. Proofs by contraposition make use of the fact that the conditional statement $p \rightarrow q$ is logically equivalent to its contrapositive, $\neg q \rightarrow \neg p$.

Example

Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

Solution

An attempt to prove this directly would lead to dead end. So instead we prove the contraposition if the statement "if $3n + 2$ *is odd, then* n *is odd", which is "if* n *is even then* $3n + 2$ *is even". So assume* n *is even, that is, there is an integer* k *such that* $n = 2k$. *Now* $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. *Therefore* $3n + 2$ *is even. This completes the proof.*

Vacuous proofs

We can quickly prove that a conditional statement $p \to q$ is true when we know that p is false, because $p \to q$ must be true when p is false. Consequently, if we can show that p is false, then we have a proof, called a vacuous proof, of the conditional statement $p \to q$.

Example

Show that the proposition $P(0)$ is true, where $P(n)$ is "If $n > 1$, then $n^2 > n$" and the domain consists of all integers.

Solution

Note that $P(0)$ is "If $0 > 1$, then $0^2 > 0$." We can show $P(0)$ using a vacuous proof. Indeed, the hypothesis $0 > 1$ is false. This tells us that $P(0)$ is automatically true.

Trivial proofs

We can also quickly prove a conditional statement $p \rightarrow q$ if we know that the conclusion q is true. By showing that q is true, it follows that $p \rightarrow q$ must also be true. A proof of $p \rightarrow q$ that uses the fact that q is true is called a trivial proof.

Example

Let $P(n)$ be "If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$," where the domain consists of all nonnegative integers. Show that $P(0)$ is true.

Solution

The proposition $P(0)$ *is "If* $a \geq b$*, then* $a^0 \geq b^0$*." Because* $a^0 = b^0 = 1$*, the conclusion of the conditional statement "If* $a \geq b$*, then* $a^0 \geq b^0$*" is true. Hence, this conditional statement, which is* $P(0)$*, is "trivially" true.*

More examples

Definition

The real number r is rational if there exist integers p and q with $q \neq 0$ such that $r = p/q$. A real number that is not rational is called irrational.

Example

Prove that the sum of two rational numbers is rational.

Solution

We first attempt a direct proof. Suppose that r and s are rational numbers. From the definition of a rational number, it follows that there are integers p and q, with $q \neq 0$, such that $r = p/q$, and integers t and u, with $u \neq 0$, such that $s = t/u$. Then

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + tq}{qu}.$$

Exercise

Prove that for any integer n, if n^2 is even then so is n.