CS 0441
Lecture 5: Proofs

KP. Wang

Overview

Overview

Proofs

- A proof is a way to derive statements from other statements.
- It starts with **axioms** (statements that are assumed in the current context always to be true), **theorems** or **lemmas** (statements that were proved already; the difference between a theorem and a lemma is whether it is intended as a final result or an intermediate tool).
- Less important theorems sometimes are called **propositions**.

- 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, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert.

Proof techniques

- A proof technique is a template for how to go about proving particular classes of statements.
- We will introduce each technique in what follows.

Vacuous and trivial 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 following the equivalent identity $\neg p \vee q$. 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 1

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.

Proof.

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. ■

- 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 2

Example

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

Proof.

The proposition $P(0)$ is "If $a \geqslant b$, then $a^0 \geqslant b^0$." Because $a^0 = b^0 = 1$, the conclusion which is $P(0)$, is true. This is an example of a trivial proof. Note that the hypothesis, which is the statement " $a \geqslant b$," was not needed in this proof. ■

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.

- To help us with the following example, we first introduce

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 3

Example

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

Proof.

First we assume that n is odd. By the definition of an odd integer, it follows that $n = 2k + 1$, where k is some integer. We want to show that n^2 is also odd. We can square both sides of the equation $n = 2k + 1$ to obtain a new equation that expresses n^2. When we do this, we find that
$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2\left(2k^2 + 2k\right) + 1$. 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). Consequently, we have proved that if n is an odd integer, then n^2 is an odd integer. ■

Proof by construction

- An important technique in direct proof is the proof by construction, namely, we need to construct certain structures based on the given conditions to complete the proof.

- Here we present another

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 4

Example

Prove that the sum of two rational numbers is rational. (Note that if we include the implicit quantifiers here, the theorem we want to prove is "For every real number r and every real number s, if r and s are rational numbers, then $r + s$ is rational.)

Proof.

We will prove by construction. To begin, 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 $s = t/u$. The obvious next step is to add $r = p/q$ and $s = t/u$, to obtain

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

Because $q \neq 0$ and $u \neq 0$, it follows that $qu \neq 0$. Consequently, we have expressed $r + s$ as the ratio of two integers, $pu + qt$ and qu, where $qu \neq 0$. This means that $r + s$ is rational. We have proved that the sum of two rational numbers is rational by construction. ■

Proof by contraposition

- Proofs by contraposition make use of the fact that the conditional statement $p \rightarrow q$ is equivalent to its contrapositive, $\neg q \rightarrow \neg p$.
- In a proof by contraposition of $p \rightarrow q$, we take $\neg q$ as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that $\neg p$ must follow.

Example 5

Example

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

Proof.

We first attempt a direct proof. To construct a direct proof, we first assume that $3n + 2$ is an odd integer. This means that $3n + 2 = 2k + 1$ for some integer k. Can we use this fact to show that n is odd? We see that $3n + 1 = 2k$, but there does not seem to be any direct way to conclude that n is odd. Because our attempt at a direct proof failed, we next try a proof by contraposition. ■

Proof.

The first step in a proof by contraposition is to assume that "If n is even, then $3n+2$ is even, where n is an integer ". Then, by the definition of an even integer, $n = 2k$ for some integer k. Substituting $2k$ for n, we find that $3n+2 = 3(2k)+2 = 6k+2 = 2(3k+1)$. This tells us that $3n+2$ is even (because it is a multiple of 2), and therefore not odd. Since the contrapositive statement is true, our proof by contraposition succeeded; we have proved the theorem "If $3n+2$ is odd, then n is odd." ■

Proof by contradiction

- Suppose we want to prove that a statement p is true. Furthermore, suppose that we can find a contradiction q such that $\neg p \rightarrow q$ is true. Because q is false, but $\neg p \rightarrow q$ is true, we can conclude that $\neg p$ is false, which means that p is true. This is what we call **a proof by contradiction**.

Example 6

Example

Let us revisit Example 5 and demonstrate it by contradiction.

Proof.

Solution: Let p be " $3n+2$ is odd" and q be " n is odd." To construct a proof by contradiction, assume that both p and $\neg q$ are true. That is, assume that $3n+2$ is odd and that n is not odd. Because n is not odd, we know that it is even. Because n is even, there is an integer k such hat $n = 2k$. This implies that $3n+2 = 3(2k)+2 = 6k+2 = 2(3k+1)$. Because $3n+2$ is $2t$, where $t = 3k+1, 3n+2$ is even. Note that the statement " $3n+2$ is even" is equivalent to he statement $\neg p$, because an integer is even if and only if it is not odd. Because both p and $\neg p$ are true, we have a contradiction. This completes the proof by contradiction, proving that if $3n+2$ is odd, then n is odd. ■

Example 7

Example

Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

Proof.

Solution: Let p be the proposition " $\sqrt{2}$ is irrational." To start a proof by contradiction, we suppose that $\neg p$ is true. Note that $\neg p$ is the statement " $\sqrt{2}$ is not irrational," namely, $\sqrt{2}$ is rational. We will show that assuming that $\neg p$ is true leads to a contradiction. ■

Proof.

If $\sqrt{2}$ is rational, there exist integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors (so that the fraction a/b is in lowest terms.) (Here, we are using the fact that every rational number can be written in lowest terms.) Because $\sqrt{2} = a/b$, when both sides of this equation are squared, it follows that

$$2 = \frac{a^2}{b^2}.$$

Hence,

$$2b^2 = a^2.$$

By the definition of an even integer it follows that a^2 is even. We next use the fact that if a^2 is even, a must also be even, which is the contrapositive statement of Example 3. ■

Proof.

Furthermore, because a is even, by the definition of an even integer, $a = 2c$ for some integer c. Thus,

$$2b^2 = 4c^2.$$

Dividing both sides of this equation by 2 gives

$$b^2 = 2c^2.$$

By the definition of even, this means that b^2 is even. Again using the fact that if the square of an integer is even, then the integer itself must be even, we conclude that b must be even as well. ■

Proof.

Note a and b being both even contradicts with our assumption that a and b have no common factors. Hence, $\neg p$ is false. That is, the statement p, "$\sqrt{2}$ is irrational," is true. We have proved that $\sqrt{2}$ is irrational. ■

Proof for equivalence

- To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true. The validity of this approach is based on the tautology

$$(p \leftrightarrow q) \equiv (p \rightarrow q) \wedge (q \rightarrow p).$$

Example 8

Example

Prove the theorem "If n is an integer, then n is odd if and only if n^2 is odd."

Proof.

Note the biconditional statement implies that we need to complete the proof from both directions. Note that n being an integer is an axiom. Let $p = n$ is odd and $q = n^2$ is odd. We need to show both $p \to q$ and $q \to p$.

Note we have completed $p \to q$ in Example 3. We are only left with proof $q \to p$. Here we show by contraposition, that is, we want to show "If n is even, then n^2 is even". It follows from the definition of evenness that there exists some integers k such that $n = 2k$. We find that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Because $2k^2$ is an integer, we know that n^2 is also even. Hence we prove by contraposition that $q \to p$.

In conclusion, we have shown both directions and the given theorem is true. ■

Remark

- You can extend the equivalence for more propositions and prove using the following identity

$$p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n \equiv (p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \cdots \wedge (p_n \rightarrow p_1)\,.$$

Proof with counterexamples

- Note that when we want to prove a statement is true, we have to follow the above techniques. But when we want to disporve a statement, that is, to prove a statement is false, we can simply find a counterexample.

Example 9

Example

Show that the statement "Every positive integer is the sum of the squares of two integers" is false.

Proof.

A counterexample is 3 because $3 = 0 + 3$ or $3 = 1 + 2$, none of which is a sum of squares of two integers. ■

Proof by exhaustion

- Some theorems can be proved by examining a relatively small number of examples. Such proofs are called **exhaustive proofs**, or **proofs by exhaustion** because these proofs proceed by exhausting all possibilities.

Example 10

Example

Prove that $(n+1)^3 \geqslant 3^n$ if n is a positive integer with $n \leqslant 4$.

Proof.

Solution: We use a proof by exhaustion. We only need verify the inequality $(n+1)^3 \geq 3^n$ when $n = 1, 2, 3$, and 4.
For $n = 1$, we have $(n+1)^3 = 2^3 = 8$ and $3^n = 3^1 = 3$;
for $n = 2$, we have $(n+1)^3 = 3^3 = 27$ and $3^n = 3^2 = 9$;
for $n = 3$, we have $(n+1)^3 = 4^3 = 64$ and $3^n = 3^3 = 27$; and for $n = 4$, we have $(n+1)^3 = 5^3 = 125$ and $3^n = 3^4 = 81$.
In each of these four cases, we see that $(n+1)^3 \geqslant 3^n$. We have used the method of exhaustion to prove that $(n+1)^3 \geqslant 3^n$ if n is a positive integer with $n \leqslant 4$. ■

Proof by cases

- A proof by cases must cover all possible cases that arise in a theorem, which can be almost viewed as a special example of the proof by exhaustion.

Example 11

Example

Prove that if n is an integer, then $n^2 \geqslant n$.

Proof.

We can prove that $n^2 \geqslant n$ for every integer by considering three cases, when $n = 0$, when $n \geqslant 1$, and when $n \leqslant -1$. We split the proof into three cases because it is straightforward to prove the result by considering zero, positive integers, and negative integers separately.

Case (i): When $n = 0$, because $0^2 = 0$, we see that $0^2 \geq 0$. It follows that $n^2 \geqslant n$ is true in this case.

Case (ii): When $n \geqslant 1$, when we multiply both sides of the inequality $n \geqslant 1$ by the positive integer n, we obtain $n \cdot n \geqslant n \cdot 1$. This implies that $n^2 \geqslant n$ for $n \geqslant 1$.

Case (iii): In this case $n \leqslant -1$. However, $n^2 \geqslant 0$. It follows that $n^2 \geqslant n$.

Because the inequality $n^2 \geqslant n$ holds in all three cases, we can conclude that if n is an integer, then $n^2 \geqslant n$. ■

Without loss of generality

- A special trick in demonstration by cases is to use the "Without loss of generality", often abbreviated as "WLOG".
- We assert that by proving one case of a theorem, no additional argument is required to prove other specified cases. This normally happens in cases where assumptions are symmetric, or some assumptions can be implied from others.

Example 12

Example

Show that if xy and $x + y$ are both even, where x and y are integers, then both x and y are even.

Proof.

We will use proof by contraposition, the notion of without loss of generality, and proof by cases. First, suppose that x and y are not both even. That is, assume that x is odd or that y is odd (or both). Without loss of generality, we assume that x is odd, so that $x = 2m + 1$ for some integer k.

To complete the proof, we need to show that xy is odd or $x + y$ is odd. Consider two cases: (i) y even, and (ii) y odd. ■

Proof.

In (i), $y = 2n$ for some integer n, so that $x + y = (2m + 1) + 2n = 2(m + n) + 1$ is odd.

In (ii), $y = 2n + 1$ for some integer n, so that $xy = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1$ is odd.

This completes the proof by contraposition. (Note that our use of without loss of generality within the proof is justified because the proof when y is odd can be obtained by simply interchanging the roles of x and y in the proof we have given.) ■

Proof with uniqueness

- In many theorems, we will see the statement involves the uniqueness, proving which normally requires two parts: existence proof and uniqueness proof.
- In more details, we can find

  Existence: We show that an element x with the desired property exists.

  Uniqueness: We show that if $y \neq x$, then y does not have the desired property. Equivalently, we can show that if x and y both have the desired property, then $x = y$.

Example 13

Example

Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Proof.

First, note that the real number $r = -b/a$ is a solution of $ar + b = 0$ because $a(-b/a) + b = -b + b = 0$. Consequently, a real number r exists for which $ar + b = 0$. This is the existence part of the proof.

Second, suppose that s is a real number such that $as + b = 0$. Then $ar + b = as + b$, where $r = -b/a$. Subtracting b from both sides, we find that $ar = as$. Dividing both sides of this last equation by a, which is nonzero, we see that $r = s$. Thlis means that if $s \neq r$, then $as + b \neq 0$. This establishes the uniqueness part of the proof.

Therefore, we complete the proof. ■