Proof Techniques

Topics

- Proof by Construction (Direct Proof)
- Indirect proof techniques
    - Proof by Contraposition
    - Proof by Contradiction
    - Proof by Counterexample

Introduction to Proofs: Terminologies

- Formally, a **theorem** is a statement that can be shown to be true. In mathematical writing, the term theorem is usually reserved for a statement that is considered at least somewhat important. Less important theorems sometimes are called **propositions**. (Theorems can also be referred to as **facts** or **results**.)
- A theorem may be the universal quantification of a conditional statement with one or more premises and a conclusion. However, it may be some other type of logical statement, as the examples later in this chapter will show.
- We demonstrate that a theorem is true with a **proof**. A proof is a valid argument that establishes the truth of a theorem.

Introduction to Proofs: Terminologies

- The statements used in a proof can include
  - **axioms** (or **postulates**), which are statements we assume to be true (for example, the axioms for the real numbers, given in Appendix 1, and the axioms of plane geometry),
  - the premises, if any, of the theorem,
  - and previously proven theorems.
- Axioms may be stated using primitive terms that do not require definition, but all other terms used in theorems and their proofs must be defined.
- 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. However, for clarity, we will often recap the statement of the theorem as the final step of a proof.

Introduction to Proofs: Terminologies

- A less important theorem that is helpful in the proof of other results is called a **lemma** (plural *lemmas* or *lemmata*).
- Complicated proofs are usually easier to understand when they are proved using a series of lemmas, where each lemma is proved individually.
- 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.
- 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.

Direct Proof: procedure

- 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.
- 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, so that the combination p true and q false never occurs.

Direct Proof: examples

For this example, we need to define even and odd integers.

- 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.

Now, give a direct proof of the theorem “If n is an odd integer, then n^2 is odd.”

Direct Proof: examples

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

Solution: To produce a direct proof of this theorem, 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, it follows that 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 must also be a perfect square when m and n are; looking ahead we see how we can show this by substituting s^2 for m and t^2 for n into mn. This tells us that $mn = s^2t^2$. Hence, $mn = s^2t^2 = (ss)(tt) = (st)(st) = (st)^2$, using commutativity and associativity of multiplication. 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. We have proved that if m and n are both perfect squares, then mn is also a perfect square.

Proof by Contraposition: procedure

- Proofs by contraposition make use of the fact that the conditional statement $p \to q$ is equivalent to its contrapositive, $\neg q \to \neg p$.
- This means that the conditional statement $p \to q$ can be proved by showing that its contrapositive, $\neg q \to \neg p$, is true.
- In a proof by contraposition of $p \to q$, 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.

Proof by Contraposition: examples

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

Solution: We first attempt a direct proof. To construct a direct proof, we first assume that $3n + 2$ is an odd integer. From the definition of an odd integer, we know 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 by Contraposition: examples

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

Because our attempt at a direct proof failed, we next try a proof by contraposition.

The first step in a proof by contraposition is to assume that the conclusion of the conditional statement “If $3n + 2$ is odd, then n is odd” is false; namely, assume that n is even. 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. This is the negation of the premise of the theorem. Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true. Our proof by contraposition succeeded; we have proved the theorem “If $3n + 2$ is odd, then n is odd.”

Proof by Contraposition: examples

Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Because there is no obvious way of showing that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ directly from the equation $n = ab$, where a and b are positive integers, we attempt a proof by contraposition. The first step in a proof by contraposition is to assume that the conclusion of the conditional statement "If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$" is false. That is, we assume that the statement $(a \leq \sqrt{n}) \vee (b \leq \sqrt{n})$ is false. Using the meaning of disjunction together with De Morgan's law, we see that this implies that both $a \leq \sqrt{n}$ and $b \leq \sqrt{n}$ are false. This implies that $a > \sqrt{n}$ and $b > \sqrt{n}$.

Proof by Contraposition: examples

Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

We can multiply these inequalities together (using the fact that if $0 < s < t$ and $0 < u < v$, then $su < tv$) to obtain $ab > \sqrt{n} \cdot \sqrt{n} = n$. This shows that $ab \neq n$, which contradicts the statement $n = ab$. Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true. Our proof by contraposition succeeded; we have proved that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proof strategy: examples

For this example, we need to define rational and irrational numbers.

- 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.

Now 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.)

Solution: We first attempt a direct proof. 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 $s = t/u$.

Proof strategy: examples

Can we use this information to show that $r + s$ is rational? That is, can we find integers v and w such that $r + s = v/w$ and $w \neq 0$? With the goal of finding these integers v and w, we add $r = p/q$ and $s = t/u$, using qu as the common denominator. We find that $r + s = p/q + t/u = (pu + qt)/qu$.

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, $v = pu + qt$ and $w = qu$, where $w \neq 0$. This means that $r + s$ is rational. We have proved that the sum of two rational numbers is rational; our attempt to find a direct proof succeeded.

Proof by Contradiction: procedure

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. How can we find a contradiction q that might help us prove that p is true in this way?

Because the statement $r \wedge \neg r$ is a contradiction whenever r is a proposition, we can prove that p is true if we can show that $\neg p \rightarrow (r \wedge \neg r)$ is true for some proposition r. Proofs of this type are called proofs by contradiction.

Proof by Contradiction: examples

Show that at least four of any 22 days must fall on the same day of the week.

Solution: Let p be the proposition “At least four of 22 chosen days fall on the same day of the week.” Suppose that $\neg p$ is true. This means that at most three of the 22 days fall on the same day of the week. Because there are seven days of the week, this implies that at most 21 days could have been chosen, as for each of the days of the week, at most three of the chosen days could fall on that day. This contradicts the premise that we have 22 days under consideration. That is, if r is the statement that 22 days are chosen, then we have shown that $\neg p \rightarrow (r \wedge \neg r)$. Consequently, we know that p is true. We have proved that at least four of 22 chosen days fall on the same day of the week.

Proof by Contradiction: examples

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

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 "It is not the case that $\sqrt{2}$ is irrational," which says that $\sqrt{2}$ is rational. We will show that assuming that $\neg p$ is true leads to a contradiction.

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 $2 = a^2/b^2$. Hence, $2b^2 = a^2$.

Proof by Contradiction: examples

Prove that √2 is irrational by giving a proof by contradiction.

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 follows by Exercise 18).

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 by Contradiction: examples

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

We have now shown that the assumption of $\neg p$ leads to the equation $\sqrt{2} = a/b$, where a and b have no common factors, but both a and b are even, that is, 2 divides both a and b. Note that the statement that $\sqrt{2} = a/b$, where a and b have no common factors, means, in particular, that 2 does not divide both a and b. Because our assumption of $\neg p$ leads to the contradiction that 2 divides both a and b and 2 does not divide both a and b, $\neg p$ must be false. That is, the statement p, "$\sqrt{2}$ is irrational," is true. We have proved that $\sqrt{2}$ is irrational.

Proof by Counterexample: procedure

- To show that a statement of the form $\forall x P(x)$ is false, we need only find a counterexample, that is, an example x for which $P(x)$ is false.
- When presented with a statement of the form $\forall x P(x)$, which we believe to be false or which has resisted all proof attempts, we look for a counterexample.

Proof by Counterexample: examples

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

Solution: To show that this statement is false, we look for a counterexample, which is a particular integer that is not the sum of the squares of two integers. It does not take long to find a counterexample, because 3 cannot be written as the sum of the squares of two integers. To show this is the case, note that the only perfect squares not exceeding 3 are $0^2 = 0$ and $1^2 = 1$. Furthermore, there is no way to get 3 as the sum of two terms each of which is 0 or 1. Consequently, we have shown that “Every positive integer is the sum of the squares of two integers” is false.