Computational Methods

PROOFS

QUOTE


BELIEVE YOU CAN
and you're halfway there.
THEODORE ROOSEVELT

Common Definitions

- A **perfect square** is an integer n such that $n = k^2$ for some integer k.
- A **prime number** is an integer $n > 1$ such that n is not divisible by any integers other than 1 and n.
- A **composite number** n is a nonprime integer; that is, $n = ab$ where a and b are integers with $1 < a < n$ and $1 < b < n$.
- For two numbers x and y, $x < y$ means $y - x > 0$.
- For two integers n and m, n **divides** m, $n \mid m$, means that m is divisible by n—that is, $m = k(n)$ for some integer k.
- The **absolute value** of a number x, $|x|$, is x if $x \geq 0$ and is $-x$ if $x < 0$.

To Prove or Not to Prove

Suppose you are doing research in some subject. You observe a number of cases in which whenever P is true, Q is also true. On the basis of these experiences, you may formulate a conjecture: $P \to Q$. The more cases you find where Q follows from P, the more confident you are in your conjecture. This process illustrates **inductive reasoning**, drawing a conclusion based on experience.

No matter how reasonable the conjecture sounds, however, you will not be satisfied until you have applied **deductive reasoning** to it as well. In this process, you try to verify the truth or falsity of your conjecture. You produce a proof of $P \to Q$ (thus making it a theorem), or else you find a **counterexample** that disproves the conjecture, a case in which P is true but Q is false.

To Prove or Not to Prove

For a positive integer n, ***n* factorial** is defined as $n(n-1)(n-2)\cdots 1$, and is denoted by $n!$. Prove or disprove the conjecture, “For every positive integer n, $n! \leq n^2$.”

Let’s begin by testing some cases:

n	$n!$	n^2	$n! \leq n^2$
1	1	1	yes
2	2	4	yes
3	6	9	yes

So far, this conjecture seems to be looking good. But for the next case,

n	$n!$	n^2	$n! \leq n^2$
4	24	16	no

we have found a counterexample. The fact that the conjecture is true for $n = 1, 2,$ and 3 does nothing to prove the conjecture, but the single case $n = 4$ is enough to disprove it.

Exhaustive Proof

While "disproof by counterexample" always works, "proof by example" seldom does. The one exception to this situation occurs when the conjecture is an assertion about a finite collection. In this case, the conjecture can be proved true by showing that it is true for each member of the collection. **Proof by exhaustion** means that all possible cases have been exhausted, although it often means that the person doing the proof is exhausted as well!

Exhaustive Proof

Prove the conjecture, "If an integer between 1 and 20 is divisible by 6, then it is also divisible by 3." ("Divisible by 6," means, "evenly divisible by 6," that is, the number is an integral multiple of 6.)

Because there is only a finite number of cases, the conjecture can be proved by simply showing it to be true for all the integers between 1 and 20. Table is the proof.

TABLE

Number	Divisible by 6	Divisible by 3
1	no	
2	no	
3	no	
4	no	
5	no	
6	yes: $6 = 1 \times 6$	yes: $6 = 2 \times 3$
7	no	
8	no	
9	no	
10	no	

Exhaustive Proof

11	no	
12	yes: $12 = 2 \times 6$	yes: $12 = 4 \times 3$
13	no	
14	no	
15	no	
16	no	
17	no	
18	yes: $18 = 3 \times 6$	yes: $18 = 6 \times 3$
19	no	
20	no	

Direct Proof

In general (where exhaustive proof won't work), how can you prove that $P \to Q$ is true? The obvious approach is the **direct proof**—assume the hypothesis P and deduce the conclusion Q. A formal proof would require a proof sequence leading from P to Q.

Following is an informal direct proof that the product of two even integers is even.

Let $x = 2m$ and $y = 2n$, where m and n are integers. Then $xy = (2m)(2n) = 2(2mn)$, where $2mn$ is an integer. Thus xy has the form $2k$, where k is an integer, and xy is therefore even.

Contraposition

If you have tried diligently but failed to produce a direct proof of your conjecture $P \rightarrow Q$, and you still feel that the conjecture is true, you might try some variants on the direct proof technique. If you can prove the theorem $Q' \rightarrow P'$, you can conclude $P \rightarrow Q$.

Prove that if the square of an integer is odd, then the integer must be odd.

The conjecture is n^2 odd $\rightarrow n$ odd. We do a proof by contraposition, and prove n even $\rightarrow n^2$ even. Let n be even. Then $n^2 = n(n)$ is even.

Contraposition

Theorems are often stated in the form "P if and only if Q," meaning P if Q and P only if Q, or $Q \rightarrow P$ and $P \rightarrow Q$. To prove such a theorem, you must prove both an implication and its converse. Again, the truth of one does not imply the truth of the other.

Prove that the product xy is odd if and only if both x and y are odd integers.

We first prove that if x and y are odd, so is xy. A direct proof will work. Suppose that both x and y are odd. Then $x = 2n + 1$ and $y = 2m + 1$, where m and n are integers. Then $xy = (2n + 1)(2m + 1) = 4nm + 2m + 2n + 1 = 2(2nm + m + n) + 1$. This has the form $2k + 1$, where k is an integer, so xy is odd.

Contraposition

A direct proof would begin with the hypothesis that xy is odd, which leaves us little more to say. A proof by contraposition works well because we'll get more useful information as hypotheses. So we will prove

$$(x \text{ odd and } y \text{ odd})' \rightarrow (xy \text{ odd})'$$

By De Morgan's law $(A \wedge B)' \Leftrightarrow A' \vee B'$, we see that this can be written as

$$x \text{ even or } y \text{ even} \rightarrow xy \text{ even} \tag{1}$$

The hypothesis "x even or y even" breaks down into three cases. We consider each case in turn.

1. x even, y odd: Here $x = 2m$, $y = 2n + 1$, and then $xy = (2m)(2n + 1) = 2(2mn + m)$, which is even.
2. x odd, y even: This works just like case 1.
3. x even, y even: Then xy is even

This completes the proof of (1) and thus of the theorem.

Contradiction

In addition to direct proof and proof by contraposition, you might use the technique of **proof by contradiction**. (Proof by contradiction is sometimes called *indirect proof*, but this term more properly means any argument that is not a direct proof.)

Therefore, in a proof by contradiction you assume that both the hypothesis and the negation of the conclusion are true and then try to deduce some contradiction from these assumptions.

Contradiction

Let's use proof by contradiction on the statement, "If a number added to itself gives itself, then the number is 0." Let x represent any number. The hypothesis is $x + x = x$ and the conclusion is $x = 0$. To do a proof by contradiction, assume $x + x = x$ and $x \neq 0$. Then $2x = x$ and $x \neq 0$. Because $x \neq 0$, we can divide both sides of the equation $2x = x$ by x and arrive at the contradiction $2 = 1$. Hence, $(x + x = x) \rightarrow (x = 0)$.

Contradiction

A well-known proof by contradiction shows that $\sqrt{2}$ is not a rational number. Recall that a **rational number** is one that can be written in the form p/q where p and q are integers, $q \neq 0$, and p and q have no common factors (other than $\pm$ 1).

Let us assume that $\sqrt{2}$ is rational. Then $\sqrt{2} = p/q$, and $2 = p^2/q^2$, or $2q^2 = p^2$. Then 2 divides p^2, so—because 2 is itself indivisible—2 must divide p. This means that 2 is a factor of p; hence 4 is a factor of p^2 , and the equation $2q^2 = p^2$ can be written as $2q^2 = 4x$, or $q^2 = 2x$. We see from this equation that 2 divides q^2 and hence 2 divides q. At this point, 2 is a factor of q and a factor of p, which contradicts the statement that p and q have no common factors. Therefore $\sqrt{2}$ is not rational.

Summary

TABLE		
Proof Technique	**Approach to Prove $P \to Q$**	**Remarks**
Exhaustive proof	Demonstrate $P \to Q$ for all possible cases.	May be used only to prove a finite number of cases.
Direct proof	Assume P, deduce Q.	The standard approach—usually the thing to try.
Proof by contraposition	Assume Q', deduce P'.	Use this if Q' as a hypothesis seems to give more ammunition than P would.
Proof by contradiction	Assume $P \wedge Q'$, deduce a contradiction.	Use this when Q says something is not true.

Mathematical Induction

FIRST PRINCIPLE OF MATHEMATICAL INDUCTION

$$\left.\begin{array}{l} 1.\ P(1) \text{ is true} \\ 2.\ (\forall k)[P(k) \text{ true} \rightarrow P(k+1) \text{ true}] \end{array}\right\} \rightarrow P(n) \text{ true for all positive integers } n$$

To prove something true for all $n \geq$ some value, think induction.

Mathematical Induction

Prove that

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$$

for any $n \geq 1$.

$P(1)$ is the equation

$$1 + 2 = 2^{1+1} - 1 \qquad \text{or} \qquad 3 = 2^2 - 1$$

which is true. We take $P(k)$

$$1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$$

as the inductive hypothesis and try to establish $P(k + 1)$:

$$1 + 2 + 2^2 + \cdots + 2^{k+1} \stackrel{?}{=} 2^{k+1+1} - 1$$

Mathematical Induction

Rewriting the sum on the left side of $P(k+1)$ reveals how the inductive assumption can be used:

$$
\begin{aligned}
&1 + 2 + 2^2 + \cdots + 2^{k+1} \\
&\quad = 1 + 2 + 2^2 + \cdots + 2^k + 2^{k+1} \\
&\quad = 2^{k+1} - 1 + 2^{k+1} && \text{(from the inductive hypothesis P}(k)) \\
&\quad = 2(2^{k+1}) - 1 && \text{(adding like terms)} \\
&\quad = 2^{k+1+1} - 1
\end{aligned}
$$

Therefore,

$$1 + 2 + 2^2 + \cdots + 2^{k+1} = 2^{k+1+1} - 1$$

which verifies $P(k+1)$ and completes the proof.

Mathematical Induction

Prove that $n^2 > 3n$ for $n \geq 4$.

Here we should use induction and begin with a basis step of $P(4)$. (Testing values of $n = 1, 2$, and 3 shows that the inequality does not hold for these values.) $P(4)$ is the inequality $4^2 > 3(4)$, or $16 > 12$, which is true. The inductive hypothesis is that $k^2 > 3k$ and that $k \geq 4$, and we want to show that $(k + 1)^2 > 3(k + 1)$.

$$
\begin{aligned}
(k + 1)^2 &= k^2 + 2k + 1 \\
&> 3k + 2k + 1 && \text{(by the inductive hypothesis)} \\
&\geq 3k + 8 + 1 && \text{(because } k \geq 4\text{)} \\
&= 3k + 9 \\
&> 3k + 3 && \text{(because } 9 > 3\text{)} \\
&= 3(k + 1)
\end{aligned}
$$

In this proof we used the fact that $3k + 9 > 3k + 3$. Of course, $3k + 9$ is greater than lots of things, but $3k + 3$ is what gives us what we want. In an induction proof, because we know exactly what we want as the result, we can let that guide us as we manipulate algebraic expressions.

Exercises

Provide counterexamples to the following statements.

a. Every geometric figure with four right angles is a square.

b. If a real number is not positive, then it must be negative.

c. All people with red hair have green eyes or are tall.

d. All people with red hair have green eyes and are tall.

Provide a counterexample to the following statement:

The number n is an odd integer if and only if $3n + 5$ is an even integer.

Exercises

Prove or disprove the given statement.

The sum of two even integers is even (do a direct proof).

The sum of two odd integers is even.

The square of an even number is divisible by 4.

The product of two irrational numbers is irrational.

Exercises

For all positive integers, let $P(n)$ be the equation

$$2 + 6 + 10 + \cdots + (4n - 2) = 2n^2$$

a. Write the equation for the base case $P(1)$ and verify that it is true.

b. Write the inductive hypothesis $P(k)$.

c. Write the equation for $P(k + 1)$.

d. Prove that $P(k + 1)$ is true.

Exercises

A *geometric progression* (*geometric sequence*) is a sequence of terms where there is an initial term a and each succeeding term is obtained by multiplying the previous term by a *common ratio* r. Prove the formula for the sum of the first n ($n \geq 1$) terms of a geometric sequence where $r \neq 1$:

$$a + ar + ar^2 + \cdots + ar^{n-1} = \frac{a - ar^n}{1 - r}$$