

## Methods of Proof

**Recall:** A **statement** or **proposition** is a sentence that is either true or false.

**Definition:** A **proof** is a convincing argument that a statement is true.

**Note:** We still use rules of inference and previously proved results when we construct proofs.

A proof **must** contain enough details to convince another person that each assertion in the proof follows from:

1. previously proved theorems
2. definitions
3. hypotheses/premises
4. rules of logic applied to the above

## Proving an Implication $P \rightarrow Q$

We first look at ways to prove a statement of this form:

If P, then Q, or:  $P \rightarrow Q$

The following proof types can also be used to prove statements of the form

$\forall x(P(x) \rightarrow Q(x))$  by applying the **rule of universal generalization**. To prove the following statement, for example:

**Theorem:** For all integers  $n$ , if  $n$  is even, then  $n^2$  is even.

So  $P(x)$ :  $x$  is even,  $Q(x)$ :  $x^2$  is even, and the statement's form is  $\forall n, P(n) \rightarrow Q(n)$  where the domain is  $\mathbb{Z}$ .

### Proof Form:

Let  $k$  be an arbitrarily chosen integer.

[... put the proof that if  $k$  is even, then  $k^2$  is even, ie the proof that  $P(k) \rightarrow Q(k)$  is true, here...]

Therefore the square of any even integer is even.  $\square$

## Proving Implications

Recall the truth table for  $P \rightarrow Q$ :

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

To prove  $P \rightarrow Q$  is true, we have to prove that Q is true whenever P is.

## Direct Proof

### First Approach to proving $P \rightarrow Q$ : Direct Proof

Assume  $P$  is true, and show  $Q$  is true.

**Example Theorem:** Let  $n$  be an integer. If  $n$  is even, then  $n^2$  is even.

How to attack the proof:

1. Do scratch work to figure out the logic of your proof before you do your final write-up.
2. Write down what is given, or what you can assume, and what your goal is.
3. You can work forward from the givens, or backwards from the goal(s), or more commonly, a combination of these approaches. This back-and-forth approach is not included in our proof write-up. The final proof is more concise and may not indicate **how** we came up with the proof.
4. Think about applying appropriate definition(s) to the givens to work forward. Or applying a definition to the goal to work backwards.
5. In the final proof, it should be obvious that every assertion in our proof came from previous assertions, hypotheses, definitions and known theorems!

**Theorem:** Let  $n$  be an integer. If  $n$  is even, then  $n^2$  is even.

**Givens:**  $n$  is even

**Goal:**  $n^2$  is even

**Scratch Work:** We start by working backwards from the goal. In steps 1 and 2, we make our goal more specific. In steps 3-5, we work forward from the given by applying the definition of even to  $n$ .

3.  $n$  is even

4.  $n = 2k$  for some integer  $k$  (applying def of even)

5.  $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$  and  $2k^2 \in \mathbb{Z}$

2. Must show:  $n^2 = 2m$  for some integer  $m$

1. Goal:  $n^2$  is even

**Proof:** Assume  $n$  is an even integer. Then by definition of even numbers,  $n = 2k$  for some integer  $k$ . So  $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ , and  $2k^2 \in \mathbb{Z}$  since  $k \in \mathbb{Z}$ . By definition of even,  $n^2$  is even.  $\square$

## Another Direct Proof Example

**Theorem:** If  $m$  and  $n$  are even integers, then  $m+n$  is even.

**Scratch Work:** exercise

**Proof:** exercise

### Alternate statement of theorem:

The sum of two even integers is even.

Translation:  $\forall m \forall n [(m \text{ is even}) \wedge (n \text{ is even}) \rightarrow (m + n \text{ is even})]$

**Proof:** Suppose  $m$  and  $n$  are arbitrarily chosen even integers. We must show that  $m+n$  is even. ... (proof is the same as before).

**Note:** To show a statement of the form  $\forall x \forall y (P(x, y) \rightarrow Q(x, y))$  is true, pick arbitrary elements  $r$  and  $z$  from the universe, assume  $P(r, z)$  is true and show  $Q(r, z)$  is true.

## More Comments on Proofs

When you are writing a proof:

1. Write in complete English sentences. Use correct grammar.
2. Do NOT write that 2 quantities are equal **unless** you have proved it!
3. Give reasons for each assertion.
4. Do not use a single example to prove a general statement. For example, you cannot prove that the sum of two even integers is even by showing that the sum  $4 + 16 = 20$  is even.
5. Do not use the same variable name to represent two different things.
6. Do not assume what you are trying to prove. For example, don't do this:

Assume  $m$  and  $n$  are even. Whenever we add two even integers, we get an even integer, so  $m+n$  is even.

**Example:** Every connected graph has a spanning tree.

Rewritten more formally:  $\forall$  graphs  $G$ , if  $G$  is connected, then  $G$  has a spanning tree.

$U =$  all graphs,  $P(G)$ :  $G$  is connected,  $Q(G)$ :  $G$  has a spanning tree.

Start the proof with: Assume  $G$  is an arbitrarily chosen graph that is connected. That is, start with an arbitrary element of the universe that satisfies the hypothesis. Then show that  $Q(G)$  is true, ie that  $Q$  is true for that arbitrarily chosen element.

## More Direct Proof Examples

**Theorem:** The product of any two odd integers is odd.

**Scratch Work and Proof:** exercise

We need a definition for the following theorem:

**Def:** For integers  $x$  and  $y$ , we say that  $x$  **divides**  $y$  if  $\exists k \in \mathbb{Z}$  such that  $kx = y$ . Notation:  $x|y$ .

**Example:**  $2|16$  since  $16 = 8 * 2$ .

**Theorem:** For all integers  $a$ ,  $b$ , and  $c$ , if  $a|b$  and  $b|c$ , then  $a|c$ .

**Proof:** Let  $a$ ,  $b$  and  $c$  be arbitrarily chosen integers. Assume that  $a|b$  and  $b|c$ . We must prove that  $a|c$ .

Since  $a|b$ ,  $b = ja$  for some integer  $j$ . Likewise, since  $b|c$ ,  $c = kb$  for some integer  $k$ . So  $c = kb = k(ja) = (kj)a$ , and  $kj$  is an integer since  $k$  and  $j$  are both integers. Therefore  $a|c$ .  $\square$

## Indirect Proof of an Implication

**Recall:** An implication  $P \rightarrow Q$  and its contrapositive statement  $\neg Q \rightarrow \neg P$  are logically equivalent. An indirect proof of  $P \rightarrow Q$  is a direct proof of the contrapositive  $\neg Q \rightarrow \neg P$ .

### Indirect Proof of $P \rightarrow Q$ :

Assume that  $Q$  is false, and prove that  $P$  is false also.

**Note:** In an indirect proof, we prove the contrapositive statement. That is, assume  $\neg Q$  is true, and show  $\neg P$  is true.

**Theorem:** If  $n^2$  is odd, then  $n$  is odd.

Contrapositive: If  $n$  is even, then  $n^2$  is even. (We already proved this).

## More on Indirect Proof

**Theorem:** A perfect number is not prime.

**Def:** A **perfect number** is an integer which is equal to the sum of all its proper divisors (ie, all divisors other than itself).

**Example:** 6 is perfect:  $6 = 1+2+3$ .

28 is also perfect. Check!

**Def:** An integer greater than 1 is **prime** if it is only divisible by 1 and itself.

**Contrapositive statement:** If an integer is prime, then it is not perfect.

**Proof:** Let  $n$  be an arbitrarily chosen integer. Assume  $n$  is prime. We must show that  $n$  is not perfect.

Since  $n$  is prime,  $n > 1$ , and  $n$ 's only divisors are 1 and  $n$ . So the sum of  $n$ 's proper divisors is 1. So  $n$  is greater than the sum of its proper divisors, and thus  $n$  is not perfect.  $\square$

## Note about Indirect Proof

Suppose the theorem has many premises:

$$(P_1 \wedge P_2 \wedge \dots \wedge P_n) \rightarrow Q.$$

The contrapositive is

$$\neg Q \rightarrow (\neg P_1 \vee \neg P_2 \vee \dots \vee \neg P_n).$$

So to do an indirect proof, we assume  $Q$  is false, and show that one hypothesis is false (ie,  $P_j$  is false for some  $j$ ).

## Proof by Contradiction

### To prove proposition **P** by contradiction:

Assume **P** is false and reach a conclusion we know is false (a contradiction).

We need a definition for the next example.

**Definition:** Every integer larger than one can be written as a product of primes.

**Theorem:** There is no largest prime number.

**Proof:** (by contradiction)

Assume by way of contradiction (BWOC) that there is a largest prime, and call this largest prime  $p$ . Since  $p$  is the largest prime, the set of primes is finite. Define  $x = (2)(3)\dots(p-1)p + 1$ . So  $x > p$ . Note that  $x$  is not evenly divisible by any integer between 2 and  $x - 1$ . Therefore the only divisors of  $x$  are 1 and  $x$  itself. Therefore  $x$  is prime. Contradiction, since  $x > p$  and  $p$  is the largest prime. Therefore our original assumption must be incorrect, and there is no largest prime number.  $\square$

### To prove $P \rightarrow Q$ by contradiction:

1. Assume **P** is true and **Q** is false.
2. Reach a contradiction.

Proof by contradiction is particularly useful when **Q** is of the form “not (something)”.

## More Proof by Contradiction

**Theorem:** Assume  $n$  is an integer. If  $n^2$  is even, then  $n$  is even.

**Proof:** Let  $n$  be an integer. Assume BWOC that the claim is false, i.e.,  $n^2$  is even and  $n$  is odd. Since  $n$  is odd,  $n = 2k + 1$  for some integer  $k$ . So  $n^2 = (2k + 1)^2 = 4k^2 + 2k + 1 = 2(2k^2 + k) + 1$ . Since  $2k^2 + k$  is an integer,  $n^2$  is odd. Contradiction, since  $n^2$  is even. Therefore the claim is true.  $\square$

We need a definition for our next theorem.

**Definition:** A real number  $r$  is **rational** if it can be expressed as  $p/q$  where  $p$  and  $q$  are integers, and  $q \neq 0$ .

**Note:** You may assume that rational number  $r$  is  $\frac{p}{q}$  where  $p$  and  $q$  have no common divisors.

**Theorem:** If  $r$  is a real number such that  $r^2 = 2$ , then  $r$  is not rational.

**Proof:** exercise

**Theorem:** There are no positive integer solutions to the equation  $x^2 - y^2 = 1$ .

**Proof:** Exercise - by contradiction