Discrete Structures
Introduction to Proofs

A Document By:
Nathan Warner

Northern Illinois University

Computer Science
Northern Illinois University
August 16, 2023
United States

Contents

Proofs

1 Terminology

- **Conjecture**: A mathematical statement that has not yet been rigorously proved but is being proposed as being true.
- **Theorem**: Is a statement that can be shown to be true, or has been shown to be true.
- **Axioms (or Postulates)**: Is a statement that is taken to be true, to serve as a premise or starting point for further reasoning and arguments.
- **Lemma**: Is a less important theorem that is helpful in the proof of theorems.
- **Corollary**: Is a theorem that can be established directly from a theorem that has been proven.

2 Direct Proof

Definition. A **direct proof** is a way of showing the truth or falsehood of a given statement by a straightforward combination of established facts, usually axioms, existing lemmas and theorems, without making any further assumptions.

Let's say we have the statement: *If n is odd number than n^2 is an odd number*

Proof: Let's assume that n is an odd number, which means that it can be expressed as $n = 2k + 1$ for some integer k. This is because odd numbers are of the form $2k + 1$ where k is an integer.

Now, let's square n:

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

As we can see from the expression $2(2k^2 + 2k) + 1$, the squared value n^2 is expressed as an even number (2 times an integer) plus 1. Since an odd number can always be represented as $2k+1$, where k is an integer, the expression $2(2k^2 + 2k) + 1$ follows the same pattern and is also an odd number.

Thus, we have shown that if n is an odd number, then n^2 is indeed an odd number. ☺

Now let's say we have the statement: *If n is even then* $(-1)^n = 1$

Proof: Let's assume that n is an even number, which means that it can be expressed as $n = 2k$ for some integer k. This is because even numbers are of the form $2k$ where k is an integer.

Now, let's consider $(-1)^{2k}$:

$$\begin{aligned}(-1)^{2k} &= ((-1)^2)^k \\ &= 1^k \\ &= 1\end{aligned}$$

Since any non-negative integer exponent of 1 is always 1, the expression $(-1)^{2k}$ simplifies to 1.

Therefore, we have shown that if n is an even number, then $(-1)^2 = 1$ holds true.

This completes the proof.

😄

For the next example, let's consider the following statement: *if $a|b$ and $a|c$, then $a|(b+c)$*, $\quad a, b, c \in \mathbb{Z}$

Proof: Assume that $a|b$ and $a|c$. This means there exist integers r and t such that:

$$\begin{aligned}b &= a \cdot r, \quad \text{(by definition of divisibility)} \\ c &= a \cdot t. \quad \text{(by definition of divisibility)}\end{aligned}$$

We want to show that $a|(b+c)$. This means there exists an integer s such that:

$$b + c = a \cdot s. \quad \text{(by definition of divisibility)}$$

Adding the equations for b and c, we get:

$$\begin{aligned}b + c &= a \cdot r + a \cdot t \\ &= a \cdot (r + t).\end{aligned}$$

Since r and t are integers, $r + t$ is also an integer. Therefore, we have shown that $b + c = a \cdot (r + t)$, which implies $a|(b+c)$. Thus, we have proved the statement.

😄

3 Proofs by Contrapositive

Recall contrapostive, if $p \to q$, then the contrapostive is $\neg q \to \neg p$. Recall that these two statements are *logically equivalent*

Definition. In mathematics, proof by contrapositive, or proof by contraposition, is a rule of inference used in proofs, where one infers a conditional statement from its contrapositive. In other words, the conclusion "if A, then B" is inferred by constructing a proof of the claim "if not B, then not A" instead. More often than not, this approach is preferred if the contrapositive is easier to prove than the original conditional statement itself.

Consider the statement: $n \in \mathbb{Z},\ if\ n^2$ *is odd, then* n *is odd*

First, let's try to prove this directly. To show that this approach is futile.

Proof: Suppose n^2 is odd. Then, we can express it as $n^2 = 2k + 1$, where k is an integer.

$$n^2 = 2k + 1, \quad k \in \mathbb{Z}.$$

Our goal is to prove that n is also odd, implying that n can be written as $n = 2k+1$, where k is an integer. Let's attempt to find a direct expression for n:

$$n = \sqrt{2k + 1}.$$

However, this doesn't provide any information about the parity of n. Therefore, a direct proof is not yielding the desired result. In such cases, we often resort to a proof by contrapositive, which can be more effective in establishing the statement. 😄

Before we begin our proof by contrapositive, let's clarify what the contrapositive is for our statement:

Statement: If n^2 is odd, then n is odd.
Contrapositive: if n is even, then n^2 is even

Proof: Suppose n is even. Then, we can express it as $n = 2k$, where k is an integer.

$$n = 2k, \quad k \in \mathbb{Z}.$$

We want to show that n^2 is also even, implying that $n^2 = 2k + 1$, where k is an integer. If we square both sides of our statement $n = 2k + 1$

$$\begin{aligned} n^2&(2k)^2 \\ n^2 &= 4k^2 \\ n^2 &= 2(2k^2). \end{aligned}$$

Since we know that if k is an integer, then k^2 must also be an integer, we have shown that the parity of n^2 is indeed even if n is even.

Therefore, by proving the contrapositive statement, we have established the original statement: If n^2 is odd, then n is odd.

😄

Let's consider another example: $\forall$ *positive real numbers,* $n \cdot m > 100$*, then* $n > 10$ *or* $m > 10$

So we have:

$$\text{Statement: } \forall \text{ positive real numbers, if } n \cdot m > 100 \text{, then } n > 10 \text{ or } m > 10$$
$$\text{Contrapostive: } \forall \text{ positive real numbers, if } n \leqslant 10 \text{ and } m \leqslant 10 \text{ then } n \cdot m \leqslant 100$$

Proof: So suppose $n \leqslant 10$ and $m \leqslant 10$, we want to show that $nm \leqslant 100$.

If:

$$\begin{aligned} &n \leqslant 10 \\ &nm \leqslant 10m \quad \text{(Multiplying both sides by m).} \end{aligned}$$

And:

$$\begin{aligned} &m \leqslant 10 \\ &10m \leqslant 100 \quad \text{(Multiplying both sides by 10).} \end{aligned}$$

Thus, it follows that:

$$nm \leqslant 100.$$

Therefore, we have shown that if $n \leqslant 10$ and $m \leqslant 10$, then nm must be $\leqslant 100$

😃