Discrete Structures
Introduction to Proofs

A Document By:
Nathan Warner

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 1. 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 2. 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 $\leqslant 100$

4 Proof by Contradiction

Definition 3. Proof by Contradiction is a form of proof that establishes the truth or the validity of a proposition, by showing that assuming the proposition to be false leads to a contradiction

Remark. There are infinitely many primes

Proof. To prove by contradiction, let's assume that there exists a *finite* number of primes

If we denote the primes

$$p_1, p_2, p_3, p_4, ..., p_n.$$

Now suppose we let some integer m be the product of these primes. Then we add one to this product

$$m = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot ... \cdot p_n + 1.$$

By the fundamental theorem of arithmetic, this new integer m must either be prime or composite. Let's explore both possibilities

Prime:

If m were to be prime, this means that we have created a new prime number. In this case, since our assumption is that there is a finite number of primes it would imply that our assumption is false, and there are indeed not a finite number of primes.

Composite:

If m were to be composite then the prime factors of m would need to be able to divide m, however, since we added one to m, we know that these prime factors will not be divisors of m. Thus, m cannot be composite

Thus, since m cannot be composite, by the fundamental theorem of arithmetic, m must be prime. This imply that there are infinitely many primes

| |

$\frown$

Remark. $\sqrt{2}$ is irrational.

Proof. For the sake of contradiction, let's assume that $\sqrt{2}$ is *rational*. If we assume that $\sqrt{2}$ is rational, then it can be expressed as:

$$\frac{a}{b}, \quad a, b \in \mathbb{Z}, \quad b \neq 0 \text{ and } \mathrm{GCF}(a, b) = 1.$$

Lemma 1: An even integer multiplied by an even integer yields an even integer.

$$\begin{aligned} \textit{Lemma } 1: \text{ Show } (2k)^2 \text{ is even for } k \in \mathbb{Z} \\ (2k)^2 \\ = 4k^2 \\ = 2(2k^2). \end{aligned}$$

Since $k \in \mathbb{Z}$, then $2k^2$ must be an integer. Which means we have the form $2k$.

$$\begin{aligned} &\sqrt{2} = \frac{a}{b} \quad \text{(by definition of rational numbers)} \\ &2 = \left(\frac{a}{b}\right)^2 \quad \text{(squaring both sides of the equation, maintaining equality)} \\ &2 = \frac{a^2}{b^2} \quad \text{(exponentiation property of fractions)} \\ &2b^2 = a^2 \quad \text{(cross multiplication property)} \\ &. \end{aligned}$$

If $2b^2$ is an even integer (by definition of an even integer), then a^2 must also be an integer. Thus, a and b must also be even integers:

$$\therefore a = 2k \text{ and } b = 2l \text{ for some integers } k, l.$$

Since $\frac{2k}{2l}$ has a GCF of 2, this implies that our statement: $\sqrt{2}$ *is rational* is false, which demonstrates a contradiction. Therefore, $\sqrt{2}$ must be irrational.

$$\begin{aligned} | \quad | \\ \frown \end{aligned}$$

😄

5 Proof by Exhaustion (Proof by cases)

Definition 4. Proof by Exhaustion the proof that something is true by showing that it is true for each and every case that could possibly be considered.

Remark. $(n+1)^3 \geqslant 3^n$, for $n \in \mathbb{N}$ and $n \leqslant 4$

Proof. To show that $(n+1)^3 \geqslant 3^n$, for $n \in \mathbb{N}$ and $n \leqslant 4$, we must show that this is true for all possible cases of n

$$\text{for } n \in (1, 2, 3, 4).$$

Case 1: $n = 1$

$$(1+1)^3 = 8 \geqslant 3^1 \quad \text{because } 8 \geqslant 3.$$

Case 2: $n = 2$

$$(2+1)^3 = 27 \geqslant 3^2 \quad \text{because } 27 \geqslant 9.$$

Case 3: $n = 3$

$$(3+1)^3 = 64 \geqslant 3^3 \quad \text{because } 64 \geqslant 27.$$

Case 4: $n = 4$

$$(4+1)^3 = 125 \geqslant 3^4 \quad \text{because } 125 \geqslant 81.$$

Thus, we have shown that $(n+1)^3 \geqslant 3^n$, for $n \in \mathbb{N}$ and $n \leqslant 4$ for every possible case of n

☺

Remark. For any positive integer x that is a perfect cube ($x = n^3$ for some positive integer n), one of the following conditions holds:

1. x is a multiple of 9 ($x = 9k$ for some positive integer k).
2. x is one less than a multiple of 9 ($x = 9k - 1$ for some positive integer k).
3. x is one more than a multiple of 9 ($x = 9k + 1$ for some positive integer k).

Proof. To show that this statement holds $\forall x \mid x = n^3,\ n \in \mathbb{Z}^+$ we will show that all three cases lead to a true statement.

First, consider any positive integer n. Since every integer can be written in the form $9p$, $9p - 1$, or $9p + 1$ for some integer p (because the remainder when dividing by 9 must be 0, 1, or -1), we will prove the three cases.

Case 1 $n = 9p$:

$$(9p)^3 = 729p^3 \qquad \text{Note: } 729p^3 = 9(81p^3) \text{ is a multiple of } 9$$

Case 2 $n = 9p - 1$:

$$(9p-1)^3 = 729p^3 - 243p^2 + 27p - 1 \qquad \text{Note: } 729p^3 - 243p^2 + 27p = 9(81p^3 - 27p^2 + 3p)$$

Therefore, $(9p - 1)^3 = 9(81p^3 - 27p^2 + 3p) - 1$ is one less than a multiple of 9.

Case 3 $n = 9p + 1$:

$$(9p+1)^3 = 729p^3 + 243p^2 + 27p + 1 \qquad \text{Note: } 729p^3 + 243p^2 + 27p = 9(81p^3 + 27p^2 + 3p)$$

Therefore, $(9p + 1)^3 = 9(81p^3 + 27p^2 + 3p) + 1$ is one more than a multiple of 9.

Therefore, it is apparent that for any positive integer x that is a perfect cube ($x = n^3$ for some positive integer n), one of the following conditions holds:

1. x is a multiple of 9 ($x = 9k$ for some positive integer k).
2. x is one less than a multiple of 9 ($x = 9k - 1$ for some positive integer k).
3. x is one more than a multiple of 9 ($x = 9k + 1$ for some positive integer k).

☺

6 Proof by Existence

Definition 5. **A proof by existence** is a proof that establishes the existence of an element with a certain desired property.

Remark. There exists a prime number p such that both $p+2$ and $p+6$ are prime numbers.

Proof. We can show that, $\exists\ p \in \mathbb{P} \mid p+2, p+6 \in \mathbb{P}$, by use of numerical methods. First, let's define a subset of $\mathbb{P}$, denoted as S, as follows:

$$S = \{2, 3, 5, 7, 11, 13\}.$$

By iterating through S, we observe that when $p = 5$, we have $p+2 = 7$ and $p+6 = 11$, where both 7 and 11 are elements of S and, by definition, prime numbers.

Thus, we have shown that there exists a prime number p such that both $p+2$ and $p+6$ are prime numbers.

Remark. $\forall x \in \mathbb{Z}\ 6x = 2k,\ k \in \mathbb{Z} \to x = 2l,\ l \in \mathbb{Z}$

Proof. We can show that $\forall x \in \mathbb{Z}\ 6x = 2k,\ k \in \mathbb{Z} \to x = 2l,\ l \in \mathbb{Z}$ finding a number x such that if x is not even when $6x$ is even.

We can start by defining a few test cases, S

$$S = \{-3, -2, -1, 0, 1, 2, 3, 4, 5\}.$$

Iterating through S we can see that when $x = 5$, x is not even when $6x$ is even

$$6(5) = 30, \quad where\ 30 = 2k\ k \in \mathbb{Z} x = 5, \quad where\ 5 = 2k+1\ k \in \mathbb{Z}$$

.

Thus, we have show that for all integers x, if $6x$ is even then x may not be even. Therefore, the remark $\forall x \in \mathbb{Z}\ 6x = 2k,\ k \in \mathbb{Z} \to x = 2l,\ l \in \mathbb{Z}$ is not a true statement for all integers x.

Proposition. $\exists\, x, y \in \bar{\mathbb{Q}} \mid x^y \in \mathbb{Q}$

Proof. To show that $\exists\, x, y \in \bar{\mathbb{Q}} \mid x^y \in \mathbb{Q}$, let's assume that $\sqrt{2}$ is irrational, then denote $x = \sqrt{2}$ and $y = \sqrt{2}$. If we want to show that x^y is a rational number when x and y are irrational, then we must compute:

$$(\sqrt{2})^{\sqrt{2}}$$

.

Since this number is clearly still irrational, lets consider when $x = (\sqrt{2})^{\sqrt{2}}$ and when $y = \sqrt{2}$. Then:

$$\begin{aligned}
x^y &= ((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} && \text{(Original expression)} \\
&= ((\sqrt{2})^{2^{\frac{1}{2}}})^{2^{\frac{1}{2}}} && \text{(Simplify } \sqrt{2} \text{ to } 2^{\frac{1}{2}}\text{)} \\
&= (\sqrt{2})^{4^{\frac{1}{2}}} && \text{(Power of a power rule, } (a^b)^c = a^{bc}\text{)} \\
&= \sqrt{2}^{\sqrt{4}} && \text{(Simplify } 4^{\frac{1}{2}} \text{ to } \sqrt{4}\text{)} \\
&= \sqrt{2}^{2} && \text{(Simplify } \sqrt{4} \text{ to } 2\text{)} \\
&= 2 && \text{(Power rule, } (\sqrt{2})^2 = 2\text{)}
\end{aligned}$$

Thus, when $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$, $x^y = 2$, where 2 is rational.

Therefore, we have shown that when $x = (\sqrt{2})^{\sqrt{2}}$ and $y = \sqrt{2}$, where x and y are irrational, then x^y is rational. Proving the proposition $\exists\, x, y \in \bar{\mathbb{Q}} \mid x^y \in \mathbb{Q}$ non-constructively

7 Proof by Uniqueness

Definition 6. To **Prove by Uniqueness** is to show that some element has some desired property, and there is only one instance.

1. Show that there exists an x with some desired property
2. Show that $y \neq x$, then y does not have a desired property

Proposition. Given $a, b \in \mathbb{R}$ and $a \neq 0$, there exists a unique $r \in \mathbb{R}$ such that $a \cdot r + b = 0$.

Proof. To prove existence, we will show that there is at least one solution r that satisfies $a \cdot r + b = 0$. Assuming $a \neq 0$, We can solve for r by isolating it in the equation:

$$\begin{aligned} a \cdot r + b &= 0 && \text{(Original equation)} \\ a \cdot r &= -b && \text{(Subtracting } b \text{ from both sides)} \\ r &= \frac{-b}{a} && \text{(Dividing both sides by } a\text{)} \end{aligned}$$

Since $a \neq 0$, the division is well-defined. Therefore, there exists at least one solution $r = \frac{-b}{a}$ that satisfies the equation.

To prove uniqueness, we will assume that there is another solution $s \neq r$ such that $a \cdot s + b = 0$. By substituting the values of r and s from the original equation, we get:

$$\begin{gathered} as + b = 0 \qquad ar + b = 0 \\ a \cdot s + b = a \cdot r + b \\ a \cdot s = a \cdot r \\ s = r \end{gathered}$$

Here, we reach a contradiction as we initially assumed that $s \neq r$, but through the proof, we derived that $s = r$. Therefore, the solution r is unique.

In conclusion, given $a, b \in \mathbb{R}$ with $a \neq 0$, there exists a unique solution $r = \frac{-b}{a}$ such that $a \cdot r + b = 0$. 😊

8 Proof by Induction

Definition 7. To **Prove by Induction** is to prove that for every n, if the statement holds for n, then it holds for n + 1

1. Basis Step: Show that $P(a)$ is true
2. Inductive Step: Show that for all integers $k \geqslant a$, if $P(k)$ is true then $P(k+1)$ is true

Proposition. $1+2+3+...+n = \frac{n(n+1)}{2}$, for $n \in \mathbb{Z}$, n $\geqslant$1

Proof. To show that $\sum\limits_{i=1}^{n} i \; = \frac{n(n+1)}{2}$, for $n \in \mathbb{Z}, n \geqslant 1$, we must first show that the basis step, when $n = 1$ that $\sum\limits_{i=1}^{1} \; i = \frac{1(1+1)}{2}$

$$\begin{aligned} 1 &= \frac{1(2)}{2} \\ 1 &= \frac{2}{2} \\ 1 &= 1. \end{aligned}$$

Assume $n = k$ holds (inductive hypothesis):

$$1+2+3+...+k = \frac{k(k+1)}{2}$$

.

Show $n = k+1$ holds:

$$\begin{aligned} 1+2+3+...+k+k+1 &= \frac{k+1(k+1+1)}{2} \\ = 1+2+3+...+k+k+1 &= \frac{k+1(k+2)}{2} \end{aligned}$$

.

By the inductive hypothesis, if $1+2+3+...+k = \frac{k(k+1)}{2}$, then it holds that:

$$\begin{aligned} \frac{k(k+1)}{2} + k + 1 &= \frac{k+1(k+2)}{2} \\ \frac{k(k+1)}{2} + k + 1 &= \frac{k^2+3k+2}{2} \\ \frac{k(k+1)}{2} + \frac{2(k+1)}{2} &= \frac{k^2+3k+2}{2} \\ \frac{k^2+k+2k+1}{2} &= \frac{k^2+3k+2}{2} \\ \therefore \frac{k^2+3k+1}{2} &= \frac{k^2+3k+2}{2} \end{aligned}$$

.

| |

⌒

😆

Proposition. 3 is a factor of $4^n + 2$

Proof. To show that 3 is a factor of $4^n + 2$, we must show that $4^n + 2 = 3r,\ r \in \mathbb{Z}$ for $P_1,\ P_k,\ and\ P_{k+1}$

Anchor: $P_1 = 4^1 + 2 = 6$, since $6 = 3(2)$, P_1 holds

Inductive hypothesis: Assume P_k holds, this implies that $4^k + 2 = 3r$, for some integer r

Inductive step: Prove P_{k+1} holds

$$\begin{aligned}
&P_{k+1} = 4^{k+1} + 2 \\
&= 4 \cdot 4k + 2 \quad \text{(by product of powers property, } x^{n+m} = x^n \cdot x^m\text{)} \\
&= (3+1) \cdot 4^k + 2 \\
&= 3 \cdot 4^k + 4^k + 2.
\end{aligned}$$

By the inductive hypothesis, $4^k + 2 = 3r$. Thus, it follows that:

$$\begin{aligned}
&3 \cdot 4^k + 3r \\
&= 3(4^k + r).
\end{aligned}$$

Therefore, we have shown that P_{k+1} has a factor of 3. Thus proving this statement by induction.

☺