Introduction to Proofs

Alvin Lin

Discrete Math for Computing: January 2017 - May 2017

Introduction to Proofs

Rough definitions/guidelines:

- A **theorem** is a statement that can be shown to be true.
- A **proposition** is a "less important" theorem.
- A **lemma** is used as a tool for proving other results.

We show that a theorem is true by using a **proof**, which is a valid argument that establishes the truth of the theorem. To prove a theorem of the form $\exists x(P(x) \rightarrow Q(x))$ we show that $P(c) \rightarrow Q(c)$ where c is an *arbitrary* element of the domain. Since c is arbitrary, we can conclude $\exists x(P(x) \rightarrow Q(x))$.

Direct Proofs

A direct proof of $p \rightarrow q$ is constructed when the first step is the assumption that p is true. Subsequent steps use rules of inference. Finally, we show that q is true.

Example

Give a direct proof of the theorem: "If an is an odd integer, then n^2 is odd".

- An integer n is **even** if there is an integer k such that $n = 2k$.
- An integer n is **odd** if there is an integer k such that $n = 2k + 1$.

- Any number is either even or odd.

$$\exists n(n = 2k + 1) \rightarrow (n^2 = 2k' + 1)$$

Proof:

- Suppose n is an odd integer.
- By definition, there is a $k \in \mathbb{Z}$ such that $n = 2k + 1$.
- Consider $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.
- $2k^2 + 2k$ is an integer, so $n^2 = 2k' + 1$ where $k' = 2k^2 + 2k$.
- Thus, n^2 is odd.

Example

Prove the theorem: "If m and n are perfect squares then nm is also a perfect square".
Definition: An integer a is a **perfect square** if there exists an integer b so that $a = b^2$.
Proof:

- Suppose m and n are arbitrary perfect squares.
- By definition, $m = s^2$, $n = t^2$ for some s and t.
- Consider $nm = s^2t^2 = (st)^2$.
- st is an integer, therefore nm is a perfect square.

Proof by Contraposition

If n is an integer and $3n + 2$ is odd, then n is odd. Proof:

- Suppose that n is an integer and $3n + 2$ is odd.
- Then $3n + 2 = 2k + 1$ for some integer k.
- Thus $3n = 2k - 1$ and $n = \frac{2k-1}{3}$, which leaves us stuck.

It is more advantageous for us to prove the contrapositive.

- Suppose that n is even. We must show that $3n + 2$ is even.
- Since n is even, $n = 2k$ for some integer k.
- This implies that $3n + 2 = 3(2k) + 2 = 2(3k + 1)$.
- Since $3k + 1$ is an integer, $3n + 2 = 2(3k + 1)$ is even.
- Thus if n is even, $3n + 2$ is even (contrapositive).

Theorem

If $n = ab$ where a, b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Proof:

- Assume $\neg(a \leq \sqrt{n} or\ b \leq \sqrt{n})$.
- Thus, $a > \sqrt{n} and\ b > \sqrt{n}$ (De Morgan's Law).
- We need to show that $n \neq ab$.
- Consider that $ab > \sqrt{n}\sqrt{n} = n$.
- Thus, $ab > n$ and $ab \neq n$.

Vacuous Proofs

We can show that $p \to q$ is true when p is false since $p \to q$ is always true when p is false. If we show that p is false, then this is called **vacuous proof**.

Example

Show that the proposition $P(0)$ is true when $P(n)$: "If $n > 1$, then $n^2 > n$" and the domain is all integers.

$P(0)$: "If $0 > 1$, then $0^2 > 0$" is true since $\neg(0 > 1)$.

Example

To prove $\exists x P(x) \to G(x)$ try to see if a direct proof is promising. If not, try a proof by contraposition.

Definition: The real number r is rational if $r = \frac{p}{q}$ where p, q are integers and $q \neq 0$.

Theorem 1: The sum of two rationals is rational.

- Assume that r and s are rational. We must show that $r+s$ is rational as well.
- $r = \frac{p}{q}; p, q \in \mathbb{Z}; q \neq 0$
- $s = \frac{t}{u}; t, u \in \mathbb{Z}; u \neq 0$
- Consider:

$$\begin{aligned} r + s &= \frac{p}{q} + \frac{t}{u} \\ &= \frac{pu + tq}{qu} \end{aligned}$$

- Since $pu + tq$ is an integer and qu is a nonzero integer, $\frac{pu+tq}{qu}$ is rational.

Theorem 2: If n is an integer, and n^2 is odd, then n is odd.

- Suppose that n is even.
- Then $n = 2k$ for some integer k.
- Thus:

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

- n^2 is even (contrapositive).

The Classic 2=1 Proof

Let:

$$\begin{aligned} a &= b \\ a^2 &= ab \\ a^2 - b^2 &= ab - b^2 \\ (a-b)(a+b) &= b(a-b) \\ a + b &= b \\ 2b &= b \\ 2 &= 1 \end{aligned}$$

This logic is flawed because we are dividing by zero. Since $a = b$, $a - b = 0$, thus step 4 is invalid.

Proof by Contradiction

Proof by contradition proves p by assuming $\neg p$ is true and showing that "something bad" happens.

To prove a statement p is true, suppose we can find a contradiction q such that $\neq p \to q$ is true. Because q is false, but $\neg p \to q$ is true, it must be that $\neg p$ is false (i.e. p is true).

Statements $r \wedge \neg r$ are contradictions whenever r is a proposition. Thus we can show p is true if $\neg p \to (r \wedge \neg r)$.

Example

Theorem: $\sqrt{2}$ is irrational.

- Assume that $\sqrt{2}$ is rational.
- Then $\sqrt{2} = \frac{p}{q}; p, q \in \mathbb{Z}; q \neq 0$ with p, q having no common factors.
- Consider:

$$\begin{aligned}(\sqrt{2})^2 &= \frac{p^2}{q^2} \\ 2 &= \frac{p^2}{q^2} \\ 2q^2 &= p^2\end{aligned}$$

- Thus p^2 is even.
- **Lemma:** If a^2 is even, then a is even.
- The lemma gives that p is even. $p = 2c; c \in \mathbb{Z}$.
- This implies that:

$$\begin{aligned}2q^2 &= (2c)^2 \\ q^2 &= 2c^2\end{aligned}$$

- By the lemma, q is even.
- This is absurd, since p and q are both even they have the factor 2 in common. This violates our assumption that they have no common factors. Thus, contradiction. $\sqrt{2}$ cannot be rational, therefore it must be rational.

Example

Given a proof by contradiction that "If $3n + 2$ is odd, then n is odd". Proof:

- Let p : "$3n + 2$ *is odd*" and q : "n *is odd*".
- Assume p and $\neg q$ are true for a proof by contradiction.
- $3n + 2$ is odd and n is even.
- By definition, $n = 2k$ for some integer k.
- Now consider $3n + 2 = 3(2k) + 2 = 2(3k + 1)$.
- Thus, $3n + 2$ is even.
- But that is a contradiction since we assumed that $3n + 2$ was odd.

Example

To prove biconditionals $p \leftrightarrow q$, we must show $p \rightarrow q$ and $q \rightarrow p$. Show that the statements are equivalent:

$$P_1 : n \textit{ is even}$$
$$P_2 : n - 1 \textit{ is odd}$$
$$P_3 : n^2 \textit{ is even}$$

We must show $p_1 \rightarrow p_2, p_2 \rightarrow p_3, p_3 \rightarrow p_1$.

$$p_1 \rightarrow p_2$$

- Assume that n is even. Then $n = 2k$ for some integer k.
- But $n - 1 = 2(k - 1) + 1$.
- Therefore, $n - 1$ is odd since $k - 1$ is an integer.
- Thus, $p_1 \rightarrow p_2$.

$$p_2 \rightarrow p_3$$

- Assume $n - 1$ is odd. Then $n - 1 = 2k + 1$ for some integer k.

- Consider:

$$\begin{aligned} n &= 2k + 2 \\ n^2 &= (2k+2)^2 \\ &= 4k^2 + 8k + 4 \\ &= 2(2k^2 + 4k + 2) \end{aligned}$$

- Thus, n^2 is even and $p_2 \to p_3$.

$$p_3 \to p_1$$

- **Contrapositive:** If n is not even, then n^2 is not even.
- Thus, n is odd, so $n = 2k + 1$ for some integer k.
- Consider:

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

- Therefore, $p_3 \to p_1$.

The statements p_1, p_2, p_3 are all equivalent.

Counterexamples

To show a statement $\exists x P(x)$ is false, it suffices to find one such x such that $P(x)$ does not hold. This x is called a **counterexample**.

Example

Prove or disprove: "Every positive integer is the sum of two squares of integers". Look for a counterexample:

- $1 = 1^2 + 0^2$
- $2 = 1^1 + 1^2$

- $3 = \ldots$

$x = 3$ is a counterexample to this proposition.

If you have any questions, comments, or concerns, please contact me at
alvin@omgimanerd.tech