The Foundations: Logic and Proofs

February 22, 2016
1.7 18 Prove that if $n$ is an integer and $3n + 2$ is even, then $n$ is even using

a  a proof by contraposition
b  a proof by contradiction
Proof

Example

To prove a theorem

\[ \forall x_1, x_2, \ldots, x_n (P(x_1, x_2, \ldots, x_n) \leftrightarrow Q(x_1, x_2, \ldots, x_n)) \]
Proof

Example
To prove a theorem

\[ \forall x_1, x_2, \ldots, x_n (P(x_1, x_2, \ldots, x_n) \leftrightarrow Q(x_1, x_2, \ldots, x_n)) \]

you must prove

\[ \forall x_1, x_2, \ldots, x_n (P(x_1, x_2, \ldots, x_n) \rightarrow Q(x_1, x_2, \ldots, x_n)) \]

and

\[ \forall x_1, x_2, \ldots, x_n (P(x_1, x_2, \ldots, x_n) \leftarrow Q(x_1, x_2, \ldots, x_n)) \]
Theorem

For all integers $n$, $n$ is odd if and only if $n - 1$ is even.

Proof.

If $n$ is odd then $n - 1$ is even.

and If $n - 1$ is even then $n$ is odd.
Proof

Biconditionals

Example

For all real numbers $x$ and all positive real numbers $d$ that $|x| < d$ if and only if $-d < x < d$. 
Existence Proofs

Example
A monk climbs a mountain with a single path in one day, sleeps in a temple atop the mountain for the night, and descends the mountain the next day. Prove that there is some time at which the monk is in the same place on both days.
Example

Prove there are two irrational numbers, $x$ and $y$ such that $x^y$ is rational.
**Existence Proofs**

**Example**

A monk climbs a mountain with a single path in one day, sleeps in a temple atop the mountain for the night, and descends the mountain the next day. Prove that there is some time at which the monk is in the same place on both days.
If $d = \min\{d_1, d_2\}$ and $x \leq d$, then $x \leq d_1$ and $x \leq d_2$.

We will need the following definition.

Defn:

$$\min\{a, b\} = \begin{cases} a & \text{if } a < b \\ a & \text{if } a = b \\ b & \text{if } b < a \end{cases}$$
Proofs

Contrapositive and Contradition

Consider proving $\forall x_1, x_2, \ldots, x_n(P(x_1, x_2, \ldots, x_n) \rightarrow Q(x_1, x_2, \ldots, x_n))$.

What is similar between proof by contraposition and proof by contradiction?
Consider proving $\forall x_1, x_2, \ldots, x_n(P(x_1, x_2, \ldots, x_n) \rightarrow Q(x_1, x_2, \ldots, x_n))$.

What is similar between proof by contraposition and proof by contradiction?

Both begin by taking $Q$ to be false.
Proofs

Contrapositive and Contradiction

Consider proving $\forall x_1, x_2, \ldots, x_n (P(x_1, x_2, \ldots, x_n) \rightarrow Q(x_1, x_2, \ldots, x_n))$.

What is similar between proof by contraposition and proof by contradiction?

Both begin by taking $Q$ to be false.

What is the difference between a proof by contrapositive and a proof by contradiction?
Proofs
Contrapositive and Contradiction

Consider proving $\forall x_1, x_2, \ldots, x_n (P(x_1, x_2, \ldots, x_n) \rightarrow Q(x_1, x_2, \ldots, x_n))$.

What is similar between proof by contraposition and proof by contradiction?

Both begin by taking $Q$ to be false.

What is the difference between a proof by contrapositive and a proof by contradiction?

In one case $\neg Q$ is the *premise* for a direct proof of $\neg P$ (proving the contrapositive of the original statement of the theorem).
In the other, $\neg Q$, possibly along with $P$, is shown to lead to a *contradiction*. $\neg Q$ is *assumed* to be true; if that leads to a contradiction, the assumption must be false. (Why?)
Proof

Biconditionals

To prove a theorem

\[ \forall x_1, x_2, \ldots, x_n (P(x_1, x_2, \ldots, x_n) \iff Q(x_1, x_2, \ldots, x_n)) \]

you must prove

\[ \forall x_1, x_2, \ldots, x_n (P(x_1, x_2, \ldots, x_n) \rightarrow Q(x_1, x_2, \ldots, x_n)) \]

and

\[ \forall x_1, x_2, \ldots, x_n (P(x_1, x_2, \ldots, x_n) \leftarrow Q(x_1, x_2, \ldots, x_n)) \]
Proof
Biconditionals

Example: Prove that

For all integers \( n \), \( n \) is odd if and only if \( n - 1 \) is even.

Thus, we must prove

\( \text{If } n \text{ is odd then } n - 1 \text{ is even.} \)

AND

\( \text{If } n - 1 \text{ is even then } n \text{ is odd.} \)
Example: Prove that

For all real numbers $x$ and all positive real numbers $d$ that $|x| < d$ if and only if $-d < x < d$.
Proofs
Where to begin

Prove: Given any number, $t$, of the form $100...01$ where the number of 0s is $3n - 1$, $n \in \mathbb{Z}^+$, prove $t$ is composite.

Identify the premises. Identify the conclusions.
Proofs
Where to begin

Prove: Given any number, \( t \), of the form 100...01 where the number of 0s is \( 3n - 1 \), \( n \in \mathbb{Z}^+ \), prove \( t \) is composite.

Identify the premises. Identify the conclusions.

\[ \forall t, \, t \in \mathbb{Z} \text{ is of the form 100...01 with } 3n - 1 \text{ 0s for } n \in \mathbb{Z}^+, \rightarrow t \text{ is composite.} \]
Proofs

Where to begin

Prove: Given any number, \( t \), of the form 100...01 where the number of 0s is \( 3n - 1 \), \( n \in \mathbb{Z}^+ \), prove \( t \) is composite.

Identify the premises. Identify the conclusions.

\( \forall t, t \in \mathbb{Z} \) is of the form 100...01 with \( 3n - 1 \) 0s for \( n \in \mathbb{Z}^+ \), \( \rightarrow \) \( t \) is composite.

What definitions do we need to review?
Proofs
Where to begin

Prove: Given any number, \( t \), of the form 100...01 where the number of 0s is \( 3n - 1 \), \( n \in \mathbb{Z}^+ \), prove \( t \) is composite.

Identify the premises. Identify the conclusions.

\( \forall t, \ t \in \mathbb{Z} \) is of the form 100...01 with 3\( n - 1 \) 0s for \( n \in \mathbb{Z}^+ \), \( \rightarrow \) \( t \) is composite.

What definitions do we need to review?

An integer, \( c \) is composite if \( \exists a, b \in \mathbb{Z} c = ab \land a \neq 1 \land b \neq 1 \).
Proof

Getting Started

\[ \forall t, t \in \mathbb{Z} \text{ is of the form } 100...01 \text{ with } 3n - 1 \text{ 0s } \rightarrow \, t \text{ is composite.} \]

\[ t = 10^{3n} + 1 \quad \text{Premise} \]
Proves

Proof

Getting Started

∀t, t ∈ ℤ is of the form 100...01 with 3n − 1 0s → t is composite.

\[ t = 10^{3n} + 1 \]  \hspace{1cm} Premise

\[ t = (10^n)^3 + 1^3 \]  \hspace{1cm} Definition exponentiation
Proof

Getting Started

\[ \forall t, t \in \mathbb{Z} \text{ is of the form } 100...01 \text{ with } 3n - 1 \text{ 0s } \rightarrow t \text{ is composite.} \]

- \[ t = 10^{3n} + 1 \] Premise
- \[ t = (10^n)^3 + 1^3 \] Definition exponentiation
- \[ t = (10^n + 1)(10^{2n} - 10^n + 1) \] Factoring \( a^3 + b^3 \)
∀t, t ∈ ℤ is of the form 100...01 with 3n − 1 0s → t is composite.

\[
\begin{align*}
t &= 10^{3n} + 1 \\
t &= (10^n)^3 + 1^3 \\
t &= (10^n + 1)(10^{2n} − 10^n + 1) \\
t \text{is composite}
\end{align*}
\]
Proof

Example: Where to begin?

Prove: If $c$ divides $a$ and $c$ divides $b$, then $c$ divides the sum of $a$ and $b$.

Premises? Conclusion?
Proof

Example: Where to begin?

Prove: If $c$ divides $a$ and $c$ divides $b$, then $c$ divides the sum of $a$ and $b$.

Premises? Conclusion?
$\forall a, b, c, c|a \land c|b \rightarrow c|(a + b)$
Definitions?

Given two positive integers, $m$ and $n$, we say $m$ divides $n$, $m|n$, if there exists positive integer $k$ such that $n = mk$. 
Proof
Where to begin

Prove: If \( n \) is a positive integer and \( n = 4 \cdot 2 \) or \( n = 4 \cdot 3 \), \( n \) is not a perfect square.
What do we do first? Second? How do we try to prove this?
Proof

Where to begin

Prove: There are infinitely many prime numbers.
Identify the *premises*. Identify the *conclusions*. Identify *definitions*. 