Book of Proof: Part III, More on Proof

January 22, 2018

If-and-Only-If Proof

Outline for If-and-Only-If Proof

Proposition P if and only if Q.

Proof.

"Only if"

[Prove $P \Rightarrow Q$ by whatever means you can.]

"If"

[Prove $Q \Rightarrow P$ by whatever means you can.]

Equivalent Statements

Theorem Suppose A is an $n \times n$ matrix. The following statements are equivalent:

a. A is invertible.

b. $Ax = b$ has a unique solution for every $b \in \mathbb{R}^n$.

c. $Ax = 0$ has only the trivial solution.

d. The reduced row echelong form of A is I_n.

e. $\det(A) \neq 0$.

f. The matrix A does not have 0 as an eigenvector.

Equivalent Statements

$$\begin{array}{ccccc} a & \Rightarrow & b & \Rightarrow & c \\ \Uparrow & & & & \Downarrow \\ f & \Leftarrow & e & \Leftarrow & d \end{array}$$

Equivalent Statements

$$\begin{array}{ccccc} a & \Rightarrow & b & \Rightarrow & c \\ \Uparrow & & & & \Downarrow \\ f & \Leftarrow & e & \Leftarrow & d \end{array}$$

$$\begin{array}{ccccc} a & \Rightarrow & b & \Leftrightarrow & c \\ \Uparrow & & \Downarrow & & \\ f & \Leftarrow & e & \Leftrightarrow & d \end{array}$$

Equivalent Statements

$$\begin{array}{ccccc} a & \Rightarrow & b & \Rightarrow & c \\ \Uparrow & & & & \Downarrow \\ f & \Leftarrow & e & \Leftarrow & d \end{array}$$

$$\begin{array}{ccccc} a & \Rightarrow & b & \Leftrightarrow & c \\ \Uparrow & & \Downarrow & & \\ f & \Leftarrow & e & \Leftrightarrow & d \end{array}$$

$$\begin{array}{ccccc} a & \Leftrightarrow & b & \Leftrightarrow & c \\ & & \Updownarrow & & \\ f & \Leftrightarrow & e & \Leftrightarrow & d \end{array}$$

Existence Proofs

Proposition There exists an even prime number.

Existence Proofs

Proposition There exists an even prime number.

Proof. Two is an even prime number. ∎

Existence Proofs

Proposition There exists an even prime number.

Proof. Two is an even prime number. ∎

Proposition There exists an integer that can be expressed as the sum of two perfect cubes in two different ways.

Existence Proofs

Proposition There exists an even prime number.
Proof. Two is an even prime number. ■

Proposition There exists an integer that can be expressed as the sum of two perfect cubes in two different ways.
Proof.

$$1^3 + 12^3 = 1729$$
$$9^3 + 10^3 = 1729$$

■

Example

Proposition 7.1 If $a, b \in \mathbb{N}$ then
there exist $k, \ell \in \mathbb{Z}$ for which $\gcd(a, b) = ak + b\ell$.

Example

Proposition 7.1 If $a, b \in \mathbb{N}$ then
there exist $k, \ell \in \mathbb{Z}$ for which $\gcd(a, b) = ak + b\ell$.

Proof. Suppose $a, b \in \mathbb{N}$.
Consider the set $A = \{ax + by : x, y \in \mathbb{Z}\}$.
A contains positive integers and 0.
Let $d \in A$ be the smallest positive integer.
$d = ak + b\ell$ for some $k, \ell \in \mathbb{Z}$.
We will show that $d = \gcd(a, b)$.
First, prove that $d \mid a$ and $d \mid b$.
Then show that it is the largest such number.

Example

Proposition 7.1 If $a, b \in \mathbb{N}$ then
there exist $k, \ell \in \mathbb{Z}$ for which $\gcd(a, b) = ak + b\ell$.

Proof (continued).
$d = ak + b\ell$ is the smallest positive element of
$A = \{ax + by : x, y \in \mathbb{Z}\}$.
Show that $d \mid a$.
Use division algorithm: $a = qd + r$.

$$\begin{aligned} r &= a - qd \\ &= a - q(ak + b\ell) \\ &= a(1 - qk) + b(-q\ell) \end{aligned}$$

So $r \in A$, $0 \leq r < d$, so $r = 0$.
So $a = qd + r = qd$ and so $d \mid a$.

Example

Proposition 7.1 If $a, b \in \mathbb{N}$ then
there exist $k, \ell \in \mathbb{Z}$ for which $\gcd(a, b) = ak + b\ell$.

Proof (continued).
$d = ak + b\ell$ is the smallest positive element of
$A = \{ax + by : x, y \in \mathbb{Z}\}$.
Show that $d \mid a$.
Use division algorithm: $a = qd + r$.

$$\begin{aligned} r &= a - qd \\ &= a - q(ak + b\ell) \\ &= a(1 - qk) + b(-q\ell) \end{aligned}$$

So $r \in A$, $0 \leq r < d$, so $r = 0$.
So $a = qd + r = qd$ and so $d \mid a$.
A similar argument shows $d \mid b$.

Example

Proposition 7.1 If $a, b \in \mathbb{N}$ then
there exist $k, \ell \in \mathbb{Z}$ for which $\gcd(a, b) = ak + b\ell$.

Proof. $d = ak + b\ell$ is the smallest positive element of $A = \{ax + by : x, y \in \mathbb{Z}\}$, and $d \mid a$ and $d \mid b$.

$$
\begin{aligned}
a &= \gcd(a, b) \cdot m \\
b &= \gcd(a, b) \cdot n \\
d &= ak + b\ell \\
&= \gcd(a, b) \cdot mk + \gcd(a, b) \cdot n\ell \\
&= \gcd(a, b)(mk + n\ell) \\
d &\geq \gcd(a, b) \\
d &= \gcd(a, b)
\end{aligned}
$$

∎

Proofs involving sets

How to show $a \in \{x : P(x)\}$

Show that $P(a)$ is true. $\blacksquare$

How to show $a \in \{x \in S : P(x)\}$

1. Verify that $a \in S$.
2. Show that $P(a)$ is true. $\blacksquare$

Proofs involving sets

How to Prove $A \subseteq B$
(Direct approach)

Proof. Suppose $a \in A$.

$\vdots$

Therefore $a \in B$. ∎

How to Prove $A \subseteq B$
(Contrapositive approach)

Proof. Suppose $a \notin B$.

$\vdots$

Therefore $a \notin A$. ∎

Proofs involving sets

How to Prove $A = B$

Proof.
[Prove that $A \subseteq B$.]
[Prove that $B \subseteq A$.]
$\blacksquare$

Disproof

How to disprove P:
Prove $\sim P$. ■

Disproof

How to disprove P:
Prove $\sim P$. ■

How to disprove $\forall x \in S, P(x)$:
Produce an example of $x \in S$ where $P(x)$ is false. ■

Disproof

How to disprove P:
Prove $\sim P$. ■

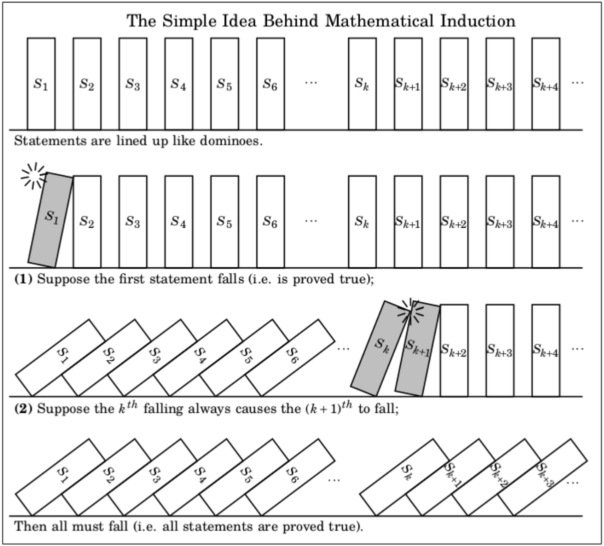
How to disprove $\forall x \in S, P(x)$:
Produce an example of $x \in S$ where $P(x)$ is false. ■

How to disprove $P(x) \Rightarrow Q(x)$:
Produce an example of x where $P(x)$ is true but $Q(x)$ is false. ■

Mathematical Induction

n	sum of the first n odd natural numbers	n^2
1	$1 =$	1
2	$1+3 =$	4
3	$1+3+5 =$	9
4	$1+3+5+7 =$	16
5	$1+3+5+7+9 =$	25
$\vdots$	$\vdots$	$\vdots$
n	$1+3+5+7+9+11+\cdots+(2n-1) =$	n^2
$\vdots$	$\vdots$	$\vdots$

Mathematical Induction



Outline for Proof by Induction

Proposition The statements $S_1, S_2, S_3, \ldots$ are all true.

Proof.

(1) Prove that S_1 is true.

(2) Prove that for $k \in \mathbb{N}$, $S_k \Rightarrow S_{k+1}$ is true. ∎

Example Proof by Induction

Proposition If $n \in \mathbb{N}$, then $1 + 3 + 5 + 7 + ... + (2n - 1) = n^2$.
(1) If $n = 1$, then we need to prove $1 = 1^2$, which is obviously true.
(2) Assume

$$1 + 3 + 5 + 7 + ... + (2k - 1) = k^2 \qquad \text{for some } k \in \mathbb{N}.$$

$$\vdots$$

Therefore,

$$1 + 3 + 5 + 7 + ... + (2(k + 1) - 1) = (k + 1)^2$$

$\blacksquare$

Example Proof by Induction

Proposition If $n \in \mathbb{N}$, then $1 + 3 + 5 + 7 + ... + (2n - 1) = n^2$.
(1) If $n = 1$, then $1 = 1^2$, which is true.
(2) Assume $1 + 3 + 5 + 7 + ... + (2k - 1) = k^2$ for some $k \in \mathbb{N}$.
Then

$$\begin{aligned} 1 + 3 + 5 + 7 + ... + 2(k + 1) - 1 &= \\ 1 + 3 + 5 + 7 + ... + (2k - 1) + (2(k + 1) - 1) &= k^2 + (2(k + 1) - 1) \\ &= k^2 + 2d + 1 \\ &= (k + 1)^2 \end{aligned}$$

Therefore,

$$1 + 3 + 5 + 7 + ... + (2(k + 1) - 1) = (k + 1)^2$$

$\blacksquare$

Example Proof by Induction

Proposition If $n \in \mathbb{N}^0$, then $5 \mid (n^5 - n)$.

Proof.

(1) If $n = 0$, then we need to prove $5 \mid (0^5 - 0)$, which is true.

(2) Assume $5 \mid (k^5 - k)$ for some $k \in \mathbb{N}^0$.

$\vdots$

Therefore $5 \mid ((k+1)^5 - (k+1))$. ■

What can we get from definitions?

Example Proof by Induction

Proposition If $n \in \mathbb{N}^0$, then $5 \mid (n^5 - n)$.
Proof.
(1) If $n = 0$, then we need to prove $5 \mid (0^5 - 0)$, which is true.
(2) Assume $5 \mid (k^5 - k)$ for some $k \in \mathbb{N}^0$.
Then $(k^5 - k) = 5a$ for some $a \in \mathbb{N}$.

$\vdots$

Then $((k+1)^5 - (k+1)) = 5b$ for some $b \in \mathbb{N}$.
Therefore $5 \mid ((k+1)^5 - (k+1))$. ■

Example Proof by Induction

Proposition If $n \in \mathbb{N}^0$, then $5 \mid (n^5 - n)$.

Proof.

(1) If $n = 0$, then we need to prove $5 \mid (0^5 - 0)$, which is true.
(2) Assume $5 \mid (k^5 - k)$ for some $k \in \mathbb{N}^0$.
Then $(k^5 - k) = 5a$ for some $a \in \mathbb{N}$.

$$
\begin{aligned}
(k+1)^5 - (k+1) &= k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1 - k - 1 \\
&= (k^5 - k) + 5k^4 + 10k^3 + 10k^2 + 5k \\
&= 5a + 5k^4 + 10k^3 + 10k^2 + 5k \\
&= 5(a + k^4 + 2k^3 + 2k^2 + k)
\end{aligned}
$$

Then $((k+1)^5 - (k+1)) = 5b$ for some $b \in \mathbb{N}$.
Therefore $5 \mid ((k+1)^5 - (k+1))$. ■

Strong Induction

Outline for Proof by Induction

Proposition The statements $S_1, S_2, S_3, \ldots$ are all true.

Proof.

(1) Prove that S_1 is true.

(2) Prove that for $k \in \mathbb{N}$, $S_k \Rightarrow S_{k+1}$ is true. ∎

Outline for Proof by Strong Induction

Proposition The statements $S_1, S_2, S_3, \ldots$ are all true.

Proof.

(1) Prove that S_1 is true. (Or the first several S_n.)

(2) Prove that for $k \in \mathbb{N}$, $(S_1 \wedge S_2 \wedge S_3 \wedge \ldots \wedge S_k) \Rightarrow S_{k+1}$ is true.

∎

Smallest Counterexample

Outline for Proof by Induction

Proposition The statements $S_1, S_2, S_3, \ldots$ are all true.

Proof.

(1) Prove that S_1 is true.

(2) Prove that for $k \in \mathbb{N}$, $S_k \Rightarrow S_{k+1}$ is true. ■

Outline for Proof by Smallest Counterexample

Proposition The statements $S_1, S_2, S_3, \ldots$ are all true.

Proof.

(1) Prove that S_1 is true.

(2) Suppose that not every S_n is true.

(3) Let S_k be the smallest false one.

(4) Then S_{k-1} is true and S_k is false.

(5) Use this to get a contradiction. ■