

1.4

Basic Proof Methods I

"A proof is a justification of the truth of a statement called a theorem."

Initial set of statements : axioms
postulates.

Your knowledge from college algebra and calculus can provide many of these.

Tautologies play a key role in proof writing

$$P \vee \neg P$$

Excluded Middle
Contrapositive

$$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$$

$$\left. \begin{aligned} P \vee (Q \vee R) &\Leftrightarrow (P \vee Q) \vee R \\ P \wedge (Q \wedge R) &\Leftrightarrow (P \wedge Q) \wedge R \end{aligned} \right\}$$

Associativity

$$\left. \begin{aligned} P \wedge (Q \vee R) &\Leftrightarrow (P \wedge Q) \vee (P \wedge R) \\ P \vee (Q \wedge R) &\Leftrightarrow (P \vee Q) \wedge (P \vee R) \end{aligned} \right\}$$

Distributivity

$$(P \Leftrightarrow Q) \Leftrightarrow (P \Rightarrow Q) \wedge (Q \Rightarrow P)$$

Biconditional

$$\neg(P \Rightarrow Q) \Rightarrow P \wedge \neg Q$$

Denial of Implication

$$\left. \begin{aligned} \neg(P \wedge Q) &\Leftrightarrow \neg P \vee \neg Q \\ \neg(P \vee Q) &\Leftrightarrow \neg P \wedge \neg Q \end{aligned} \right\}$$

De Morgan's Laws

$$P \Leftrightarrow (\neg P \Rightarrow (Q \wedge \neg Q))$$

Contradiction

$$[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$$

Transitivity

$$[P \wedge (P \Rightarrow Q)] \Rightarrow Q$$

(Modus Ponens.)

- A sentence whose symbolic translation is a tautology may be used at any time in a proof.
- some tautologies are justifications for proof techniques.

Modus Ponens

If both statement P and statement $P \Rightarrow Q$ have been deduced earlier in a proof, we may deduce that Q is true.

Ex: If today is Friday, then I will go to work.
Today is Friday. Therefore, I will go to work.

Ex: You are at a crime scene and have established the following facts:

- 1) If the crime did not take place in the Billiard room, then Colonel Mustard is guilty.
- 2) The lead pipe is not the ^{not} weapon
- 3) Either Colonel Mustard is ^{not} guilty or the weapon used was a lead pipe.

Use logic!

- (1) $\sim B \Rightarrow M$
- (2) $\sim L$
- (3) $\sim M \vee L$

B = Billiard room

M = Mustard is guilty

L = Lead pipe is weapon

$[(\sim B \Rightarrow M) \wedge \sim L \wedge (\sim M \vee L)] \Rightarrow B$ is a tautology!

Therefore the crime took place in the billiard room!

$\sim L$ is true. Therefore, $\underbrace{\sim M \vee L \Rightarrow \sim M}_{\text{a tautology.}}$

$\sim L$	M	$\sim M$	L	$\sim M \vee L$	$\sim M \vee L \Rightarrow \sim M$
T	T	F	F	F	T
T	F	T	F	T	T

Since $\sim B \Rightarrow M$, then $\sim M \Rightarrow B$.

Therefore, $\sim L \Rightarrow (\sim M \vee L \Rightarrow \sim M) \Rightarrow B$.

You can also form the truth table for the entire thing:

$$(\sim B \Rightarrow M) \wedge \sim L \wedge (\sim M \vee L)$$

L	$\sim L$	B	$\sim B$	M	$\sim M$	$\sim B \Rightarrow M$	$\sim M \vee L$	conjunction!	conjunction $\Rightarrow B$
F	T	T	F	T	F	T	F	F	T
F	T	T	F	F	T	T	T	T	T
F	T	F	T	T	F	T	F	F	T
F	T	F	T	F	T	F	T	F	T
T	F	T	F	T	F	T	T	F	T
T	F	T	F	F	T	T	T	F	T
T	F	F	T	T	F	T	T	F	T
T	F	F	T	F	T	F	T	F	T

Not needed
Since $\sim L$ is true!

It must be that

$$(\sim B \Rightarrow M) \wedge \sim L \wedge (\sim M \vee L) \Rightarrow B.$$

Therefore, the crime was committed in the
billiard room!

Direct Proof of $P \Rightarrow Q$

Proof:

Assume P .

$\vdots$

Therefore, Q

Thus, $P \Rightarrow Q$.

Ex: Suppose $\mu = E(X)$ and $E(ag(X)+b) = aE(g(X))+b$.

Prove that $\text{Var}(X) = E[(X-\mu)^2] = E(X^2) - \mu^2$

Proof:

$$\text{Var}(X) = E[(X-\mu)^2]$$

$$\Leftrightarrow \text{Var}(X) = E[X^2 - 2\mu X + \mu^2]$$

$$\Leftrightarrow \text{Var}(X) = E[X^2] - 2\mu E[X] + \mu^2 \quad (\text{Since } E(aX+b) = aE(X)+b)$$

$$\Leftrightarrow \text{Var}(X) = E(X^2) - 2\mu(\mu) + \mu^2$$

$$\Leftrightarrow \text{Var}(X) = E(X^2) - \mu^2$$

Therefore,

$$\text{Var}(X) = E(X-\mu)^2 = E(X^2) - \mu^2$$

Note, these all follow these steps.

- 1) Determine precisely the hypotheses (if any) and the antecedent & consequent.
- 2) Replace (if necessary) the antecedent with a more usable equiv.
- 3) Replace the consequent (if necessary) by something equiv & more readily shown.
- 4) Develop a chain of statements, each deducible from its predecessors that leads from the antecedent to the consequent.

○ Make sure each step is a complete sentence!
Include important connective words.

Proof by exhaustion — examines every possible case.

— Four color thm.

→ π from area of a polygon

Ex: Let x be an integer. Prove that if x is odd, then $x+1$ is even.

Proof:

Suppose x is an integer and is odd. It follows that $x = 2k+1$, where k is an integer.

Since $x+1 = 2k+1+1 = 2k+2 = 2(k+1)$ is a multiple of 2, it follows that $x+1$ is even!

Therefore, if x is odd, then $x+1$ is even.

Ex: Suppose a, b, c are integers. Prove that if a divides b and b divides c , then a divides c .

Proof:

Let a, b, c be integers. Suppose a divides b and b divides c . Then there exists integers k, n such that $b = ak$ and $c = bn$.

It therefore follows that

$$c = bn = akn$$

Since k & n are integers, then $\frac{c}{a} = kn$ is an integer. It follows that a divides c .

Therefore, if a divides b , and b divides c , then it follows that a divides c .