Module 3.5: Proofs by Contradiction

MCIT Online - CIT592 - Professor Val Tannen

Lecture Notes

Proofs by contradiction I

A statement of the form "P and (not P)" is called a **contradiction**. It is always **false**. In what follows C stands for a statement that is a contradiction.

Proof pattern. To prove "P" we can instead prove "if (not P) then C".

This proof pattern is justified by the following logical equivalence:

$$. \quad p \equiv \neg p \Rightarrow \mathtt{F}.$$

(Yes, $\mathtt{F}$, and $\mathtt{T}$, are also boolean expressions.)

We verify this logical equivalence with a truth table:

p	$\neg p$	$\neg p \Rightarrow \mathtt{F}$
$\mathtt{T}$	$\mathtt{F}$	$\mathtt{T}$
$\mathtt{F}$	$\mathtt{T}$	$\mathtt{F}$

Proofs by contradiction II

Proof pattern (variant). To prove "if P then Q" we can instead prove "if P and (not Q) then C".

This proof pattern is justified by the following logical equivalence:

$$. \quad p \Rightarrow q \quad \equiv \quad p \wedge \neg q \Rightarrow \mathrm{F}$$

We also verify this logical equivalence with a truth table:

p	q	$p \Rightarrow q$	$\neg q$	$p \wedge \neg q$	$p \wedge \neg q \Rightarrow \mathrm{F}$
T	T	T	F	F	T
T	F	F	T	T	F
F	T	T	F	F	T
F	F	T	T	F	T

Quiz

Is $p \wedge q \Rightarrow r$ logically equivalent to $p \Rightarrow (q \Rightarrow r)$? Before you answer, construct the truth table to see if they are logically equivalent.

A. Yes.

B. No.

Answer

Is $p \wedge q \Rightarrow r$ logically equivalent to $p \Rightarrow (q \Rightarrow r)$?

A. Yes.

   Correct. Refer to the truth table below.

B. No.

   Incorrect.

More Information

This is the complete truth table for the question above.

p	q	r	$p \wedge q$	$(p \wedge q) \Rightarrow r$	$q \Rightarrow r$	$p \Rightarrow (q \Rightarrow r)$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	T	T	T
T	F	F	F	T	T	T
F	T	T	F	T	T	T
F	T	F	F	T	F	T
F	F	T	F	T	T	T
F	F	F	F	T	T	T

A proof by contradiction

Problem. Prove that if $3n + 2$ is odd then n is odd.

Answer. Assume (toward a contradiction) that $3n + 2$ is odd but n is even.

Then there exists an integer k such that $n = 2k$.

Therefore we can write $3n + 2 = 3(2k) + 2 = 2(3k + 1)$

Since k is an integer, clearly $3k + 1$ is an integer.

Thus $3n + 2$ is even, by definition.

This contradicts the assumption that $3n + 2$ is odd.

(We have proven that $3n + 2$ is both even and odd!)

Square root of 2 is irrational I

Problem. Prove that $\sqrt{2}$ is not rational.

Answer. Assume (toward a contradiction) that $\sqrt{2}$ is rational.

Then $\sqrt{2}$ can be expressed as a fraction $\sqrt{2} = \frac{a}{b}$.
with $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$.

Moreover, we can assume **without loss of generality** (abbreviation w.l.o.g.) that a and b have no common divisors (factors) other than 1. Then

$$
\begin{aligned}
2 &= \frac{a^2}{b^2} && \text{(Squaring both sides)} \\
a^2 &= 2b^2 && \text{(Multiplying both sides by 2)}
\end{aligned}
$$

From the second equality it follows that a^2 is even.

Square root of 2 is irrational II

Lemma. Let z be an integer. If z^2 is even then z is even.

Proof of Lemma. We prove the contrapositive: if z is odd then z^2 is odd.
Assume that z is odd.

Then $z = 2k + 1$ for some integer k.

Then $z^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

Therefore z^2 is also odd.

Square root of 2 is irrational III

Problem. Prove that $\sqrt{2}$ is not rational.

Answer (continued). The last two statements we have shown were

$$a^2 = 2b^2 \qquad \text{and} \qquad a^2 \text{ is even.}$$

By the Lemma a is also even. That is, for some integer k, $a = 2k$.

$$\begin{aligned} a^2 &= 4k^2 && \text{(Squaring both sides)} \\ 4k^2 &= 2b^2 && \text{(Using } a^2 = 2b^2\text{)} \\ 2k^2 &= b^2 && \text{(Dividing by 2)} \end{aligned}$$

Hence b^2 is even and by the Lemma, b is even.

Therefore both a and b are even and this **contradicts** the assumption that a and b have no common factors except 1.

Penn Engineering

Activity : Proof techniques

Lemma: Let z be an integer. If z^2 is even then z is even.

Recall that we just proved this lemma by contrapositive. In this activity, we are going to prove the same lemma by contradiction.

In fact, any proof by contrapositive of $p \Rightarrow q$ can be transformed into a proof by contradiction that follows the variant pattern. We'll walk through this transformation using the example above.

Assume p. In this example, we assume that z^2 is even.

Assume toward a contradiction that $\neg q$. In this example we assume toward a contradiction that z is odd.

Activity : Proof techniques (Continued)

Now we insert the proof for the contrapositive $\neg q \Rightarrow \neg p$.

This is the same proof we saw in this segment:

If z is odd, then by definition of odd, $z = 2k + 1$ for some integer k.

Then by squaring both sides,

$$z^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

Question: At this point what can we conclude?

In the video, there is a box here for learners to put in an answer to the question above. As you read these notes, try it yourself using pen and paper!

Activity : Proof Techniques (Continued)

Answer:

Therefore z^2 is also odd.

Observe that we have derived $\neg p$ for this example.

Now you have reached a contradiction between $\neg p$ and p.

More generally, this activity demonstrates that any proof by contrapositive can be converted into a proof by contradiction.