Notes on Proof By Contradiction and Proof By Contraposition*

Hyunyoung Lee

January 22, 2016

In this short lecture note, I will explain the difference between proof by contraposition and proof by contradiction, which seem to cause some confusions easily. The basic concept is that proof by contraposition relies on the fact that $p \rightarrow q$ and its contraposition $\neg q \rightarrow \neg p$ are logically equivalent, thus, if $p(x) \rightarrow q(x)$ is true for all $x$ then $\neg q(x) \rightarrow \neg p(x)$ is also true for all $x$, vice versa. On the other hand, proof by contradiction relies on the simple fact that if the given theorem $P$ is true, the $\neg P$ is not true. This proof method is applied when the negation of the theorem statement is easier to be shown to lead an absurd (not true) situation.

To demonstrate the difference between the two proof methods, let us consider the following theorem:

**Theorem 1.** For all integers $n$, if $n^2$ is even then $n$ is even.

Let $P$ be the above theorem, then, $P$ is of the following structure:

$$\forall n \in \mathbb{Z} \,(p(n) \rightarrow q(n))$$

where $p(n)$ is the statement “$n^2$ is even” and $q(n)$ is “$n$ is even.”

**Proof by contraposition.** To prove $P$ is true by contraposition, we prove the following statement:

$$\forall n \in \mathbb{Z} \, \((\neg q(n) \rightarrow \neg p(n))$$

*For Students in CSCE 222 [Sections 201, 501 and 502], Spring 2016*
because if \( p(n) \rightarrow q(n) \) holds for all integers \( n \), then \( \neg q(n) \rightarrow \neg p(n) \) also holds for all integers \( n \).

Now, we have \( \neg q(n) = \text{“} n \text{ is not even} \text{”} \), thus \( n \) is odd, then, \( n = 2k + 1 \) for some integer \( k \) by definition of an odd integer. Then, \( n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \), and we know that \( 2k^2 + 2k \) is also an integer, therefore, \( n^2 \) is also an odd integer. Thus, we showed that “for all integers \( n \), if \( n \) is not even then \( n^2 \) is not even,” hence, we proved that \( \forall n \in \mathbb{Z} (\neg q(n) \rightarrow \neg p(n)) \equiv \forall n \in \mathbb{Z} (p(n) \rightarrow q(n)) \), which is \( p \).

**Proof by contradiction.** To prove \( P \) is true by contradiction, we assume for contradiction that \( \neg P \) is true. Then, we have

\[
\neg P = \neg \forall n \in \mathbb{Z} (p(n) \rightarrow q(n))
\]

\[
\equiv \exists n \in \mathbb{Z} \neg (p(n) \rightarrow q(n)) \quad \text{By De Morgan’s Law}
\]

\[
\equiv \exists n \in \mathbb{Z} (\neg p(n) \lor q(n)) \quad \text{By Logical Equivalence}
\]

\[
\equiv \exists n \in \mathbb{Z} (\neg \neg p(n) \land \neg q(n)) \quad \text{By De Morgan’s Law}
\]

\[
\equiv \exists n \in \mathbb{Z} (p(n) \land \neg q(n)) \quad \text{By Double Negation Law}
\]

Thus, we are assuming for contradiction that

\( \neg P = \text{“} \text{For some integer } n, n^2 \text{ is even but } n \text{ is not even.} \text{”} \) \hspace{1cm} (1)

Since \( n \) is not even, \( n \) is odd, which gives us \( n = 2k + 1 \) for some integer \( k \) by definition of an odd integer. Then, \( n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \), and we know that \( 2k^2 + 2k \) is also an integer, therefore, \( n^2 \) is also an odd integer. However, this contradicts that “\( n^2 \) is even” in (1) above, therefore \( \neg P \) is false, thus proving that \( P \), the original theorem statement, is true.