Notes on Proof by Contrapositive and Proof by Contradiction

Hyunyoung Lee

August 29, 2019

In this short lecture note, I explain the difference between proof by contrapositive and proof by contradiction. The basic concept is that proof by contrapositive relies on the fact that $p \to q$ and its contrapositive $\neg q \to \neg p$ are logically equivalent, thus, if $p(x) \to q(x)$ is true for all x then $\neg q(x) \to \neg p(x)$ is also true for all x, and vice versa. This proof method is used when, in order to prove that $p(x) \to q(x)$ holds for all x, proving that its contrapositive statement $\neg q(x) \to \neg p(x)$ holds for all x is easier.

Proof by contradiction relies on the simple fact that if the given theorem P is true, then $\neg P$ is false. This proof method is applied when the negation of the theorem statement is easier to be shown to lead to an absurd (not true) situation than proving the original theorem statement using a direct proof.

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 can be written as a quantified predicate as follows.

$$\forall n \in \mathbf{Z}\,(p(n) \to q(n))$$

where the domain for n is the set of integers, $p(n)$ is the statement "n^2 is even", and $q(n)$ the statement "n is even."

Proof by contrapositive. To prove that P is true by contrapositive, we prove the following statement:

$$\forall n \in \mathbf{Z}\,(\neg q(n) \to \neg p(n))$$

because if $p(n) \to q(n)$ holds for all integers n, then $\neg q(n) \to \neg p(n)$ also holds for all integers n.

Now, we have $\neg q(n) =$ "n is not even", thus n is odd, thus, $n = 2k + 1$ 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 an odd integer. Thus, we showed that "for all integers n, if n is not even then n^2 is not even," hence, proved that $\forall n \in \mathbf{Z}\,(\neg q(n) \to \neg p(n))$ holds, proving that $\forall n \in \mathbf{Z}\,(p(n) \to q(n))$ holds, which is the given theorem.

Proof by contradiction. To prove that the given theorem P is true by contradiction, we start out by assuming *for contradiction* that $\neg P$ is true. Then, we will come to that $\neg P$ cannot be true (reaching a contradiction), thus the given theorem P must be true.

Here is the proof (by contradiction): Let us assume for contradiction that $\neg P$ is true, thus we have

$$\begin{aligned}
\neg P &= \neg \forall n \in \mathbf{Z}\,(p(n) \to q(n)) \\
&\equiv \exists n \in \mathbf{Z} \neg\,(p(n) \to q(n)) \quad \text{By de Morgan's law} \\
&\equiv \exists n \in \mathbf{Z} \neg\,(\neg p(n) \lor q(n)) \quad \text{By the implication law} \\
&\equiv \exists n \in \mathbf{Z}\,(\neg\neg p(n) \land \neg q(n)) \quad \text{By de Morgan's law} \\
&\equiv \exists n \in \mathbf{Z}\,(p(n) \land \neg q(n)) \quad \text{By double negation law}
\end{aligned}$$

Thus, we are assuming for contradiction that

$$\neg P = \text{"For some integer } n,\ n^2 \text{ is even but } n \text{ is not even."} \tag{1}$$

The statement in (1) means that there exists some integer n that makes both of the two statements "n^2 is even" and "n is not even" true. Since n is not even, n is odd, so $n = 2k + 1$ for some integer k by definition of an odd integer. Now, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, and we know that $2k^2 + 2k$ is also an integer, therefore, n^2 is an odd integer. However, this contradicts our supposition in (1) that there exists such integer n that makes the conjunction "n^2 is even" and "n is not even" to be true. Therefore $\neg P$ is false, hence P, the original theorem statement, is true.

Have fun!