Lecture 6

In the last lecture we discussed two particular Proof Techniques, namely **Indirect Proof** *and* **Induction**. *In this lecture, we discuss an important third Proof Technique, called the* **Contrapositive Method**. *Mathematicians also speak often about* **necessary** *and* **sufficient conditions**. *We will have a closed look at this.*

Before we discuss the Contrapositive Method, let us again start with a bit of logic:

We show that the following two statements are equivalent: "A $\Rightarrow$ B" and "(not B) $\Rightarrow$ (not A)":

A	B	not A	not B	A $\Rightarrow$ B	(not B) $\Rightarrow$ (not A)
False	False	True	True	True	True
False	True	True	False	True	True
True	False	False	True	False	False
True	True	False	False	True	True

The two statements "A $\Rightarrow$ B" and "(not B) $\Rightarrow$ (not A)" are called **contrapositive statements"**. The principle of contrapositive statements is very useful for a proof technique, called Contrapositive Method. Let us look again at an indirect proof of the last seminar:

Proposition 1. *Let $x, y \in \mathbb{N}$ and $x > y$. If $2y+1$ is not a prime then $x^2 - y^2$ is also not a prime.*

The indirect proof started with: Assume $2y+1$ is not a prime and $x^2 - y^2$ is a prime. This assumption leads to a **Contradiction**!

The contrapositive of the above statement is

Proposition 2. *Let $x, y \in \mathbb{N}$ and $x > y$. If $x^2 - y^2$ is a prime then $2y + 1$ is also a prime.*

Another way of proving Proposition 1 is to prove its contrapositive statement (Proposition 2) directly. We call this method the **Contrapositive Method**.

Contrapositive Proof Method for Proposition 1: Let $x^2 - y^2$ be prime. Since $x^2 - y^2 = (x - y)(x + y)$, we must have $x - y = 1$ and $x + y = x^2 - y^2$. This leads to $x^2 - y^2 = x + y = (y + 1) + y = 2y + 1$, i.e., $2y + 1$ is a prime number. □

But be careful: Do not confuse the **Contrapositive Statement** of "If A then B" with "If not A then not B". Here is an example to see that the first statement can be true while the second is false, so these statements are **not equivalent**: "If $x = 2$ then x is even" is TRUE, but "If $x \neq 2$ then x is not even" is FALSE. (But the contrapositive statement "If x is not even then $x \neq 2$" is TRUE!)

Another Example for the Contrapositive Method:

Lemma. *Let $x \in \mathbb{N}$. If x^2 is even then x is also even.*

Proof: The contrapositive is "If x is not even (i.e., odd) then x^2 is not even (i.e., odd)". We prove this directly. Assume that x is odd, i.e., $x = 2k-1$ with $k \in \mathbb{N}$. Then

$$x^2 = (2k-1)^2 = 4k^2 - 4k + 1 = 2(2k^2 - 2k) + 1,$$

i.e., x^2 is also odd. □

Now we will discuss necessary and sufficient conditions:

Definition. *A* **necessary condition** *is one which must be satisfied so that a statement is true. A* **sufficient condition** *is one which guarantees that a statement is true.*

Here are some examples: Let $f : \mathbb{R} \to \mathbb{R}$ be a function which is infinitely many times differentiable. $x_0 \in \mathbb{R}$ is called **local minimum** of f if there exists $\epsilon > 0$ and a little interval $I := (x_0 - \epsilon, x_0 + \epsilon) \subset \mathbb{R}$ so that $f(x) \geq f(x_0)$ for all $x \in I$.

(a) A **necessary** condition for x_0 to be a local minimum of f is $f'(x_0) = 0$. But this condition is **not sufficient**.

Explanation: If $f'(x_0) \neq 0$ then f would be strictly increasing or decreasing in a neighbourhood of x_0, i.e., x_0 could not be a local minimum. Therefore $f'(x_0) = 0$ is necessary for x_0 to be a local minimum. For $f(x) = x^3$, we have $f'(0) = 0$, but $x_0 = 0$ is not a local minimum. Therefore $f'(x_0) = 0$ is not sufficient for x_0 to be a local minimum.

(b) A **sufficient** condition for x_0 to be a local minimum of f is ($f'(x_0) = 0$ and $f''(x_0) > 0$). But this condition is **not necessary**.

Explanation: $f''(x_0) > 0$ means that f' is strictly increasing in a small enough interval $I = (x_0 - \epsilon, x_0 + \epsilon)$. Since $f'(x_0) = 0$, we know that

$f(x)$ is strictly decreasing for $x \in I$ and $x < x_0$, and strictly increasing for $x \in I$ and $x > x_0$. Therefore x_0 must be a local minimum. For $f(x) = x^4$, $x_0 = 0$ is a local minimum (even a global minimum), but we have $f'(0) = 0$ and $f''(0) = 0$. Therefore $(f'(x_0) = 0$ and $f''(x_0) > 0)$ is not a necessary condition.

For the next example, let us recall the notions of **injectivity** and **surjectivity**. Here are the definitions:

Definition. *Let X, Y be two sets and $f : X \to Y$ be a map. f is called* injective*, if*

$$\forall x_1, x_2 \in X, x_1 \neq x_2 : f(x_1) \neq f(x_2).$$

f is called surjective*, if*

$$\forall y \in Y \exists x \in X : y = f(x).$$

f is called **bijective** *or* **one to one***, if f is both injective and surjective.*

Here is our next example: Let $N, M \in \mathbb{N}$ and $X := \{1, 2, \ldots, N\}$ and $Y := \{1, 2, \ldots, M\}$, and $f : X \to Y$ be a map. Then

(a) $N < M$ is a **sufficient** condition for f to be **not surjective**.
Explanation: Since f maps every element of X to just one element in Y, there number of elements in the image of f

$$f(X) := \{f(k) \mid k \in X\} \subset Y$$

is less or equal to N. But the set Y contains $M > N$ elements, so not all elements of Y can be in the image of f, i.e., f is not surjective.

(b) $N \leq M$ is a **necessary** condition for f to be **injective**.
Explanation: If f is injective, then different elements of X must be mapped to different elements of Y under f. This means that the number of elements in Y cannot be smaller than the number of elements in X, i.e., $M = |Y| \geq |X| = N$. But be aware: $N \leq M$ does not imply that f is injective, i.e., $N \leq M$ is not sufficient for f to be injective. An example of a non-injective function satisfying this condition is $f : \{1, 2\} \to \{1, 2, 3, 4\}$ with $f(1) = f(2) = 2$.