CS 173, notes from September 11, 2018

These notes show two ways of proving theorems - one by induction and the other by contradiction.

Theorem 1: Let $F : \mathbb{Z}^+ \to \mathbb{Z}$ be defined recursively by

- $F(1) = 3$
- $F(n) = 2F(n-1) + 1$ for $n \geq 2$

Then $F(n) > 2^{n-1}$ for all $n \in \mathbb{Z}^+$.

Proof 1: The proof is by contradiction. Let $P(n)$ be the assertion that $F(n) > 2^{n-1}$. Suppose it is not the case that $P(n)$ is true for all positive integers n. Then there is at least one positive integer where $P(n)$ is false. Let N be the first such positive integer. Hence $F(N) \leq 2^{N-1}$ and $N \geq 1$.

We first check if $N = 1$ is possible. By the definition of the function, $F(1) = 3$ and $3 > 2^{1-1} = 2^0 = 1$. Hence $P(1)$ is true, and so $N = 1$ is not possible. Therefore N must be at least 2.

Since $N \geq 2$, by the definition of the function, we see that

$$F(N) = 2F(N-1) + 1.$$

Note that $N - 1 \geq 1$ (becuase $N \geq 2$) and so $P(N-1)$ is true (because N is the smallest positive integer n for which $P(n)$ is false). Therefore

$$F(N-1) > 2^{N-2}.$$

Putting these together, we obtain

$$F(N) = 2F(N-1) + 1 > 2 \times 2^{N-1} + 1 = 2^N + 1 > 2^N.$$

In other words, we have shown that $P(N)$ is also true. Thus, we derived a contradiction, and so the statement $P(n)$ must be true for all positive integers n. Q.E.D.

Proof 2: The second proof is by induction on n. Let $P(n)$ be as in the previous proof, and note that we have already established that $P(1)$ is true.

Let N be an arbitrary positive integer. Our Inductive hypothesis is that $P(N)$ is true, and we wish to derive that $P(N+1)$ is true. In other words, we wish to derive that $F(N+1) > 2^N$.

Since $N \geq 1$, it follows that $N + 1 \geq 2$, and hence by the definition of the function F, we obtain:

$$F(N+1) = 2F(N) + 1$$

By our I.H., $F(N) > 2^{N-1}$, and so

$$F(N+1) = 2F(N) + 1 > 2 \times 2^{N-1} + 1 = 2^N + 1 > 2^N$$

In other words, we have shown that

$$F(N+1) > 2^N$$

and thus $P(N+1)$ is true.

Since N was an arbitrary positive integer, this means we have shown that $P(n)$ is true for all positive integers n. Q.E.D.