Module 2.5: Two Basic Proof Patterns

MCIT Online - CIT592 - Professor Val Tannen

Lecture Notes

Proof of an "if-then" statement

Recall the statement

If $m + n$ is even then $m - n$ is even.

Logical structure: $\mathit{even}(m + n) \Rightarrow \mathit{even}(m - n)$.

What did we do?

We assumed the premise $\mathit{even}(m + n)$.

Then, $m + n = 2\ell$, for some integer ℓ (by definition of "even").

Then, $m = 2\ell - n$.

Then, $m - n = (2\ell - n) - n = 2\ell - 2n = 2(\ell - n)$.

Then, we satisfied the definition of "even" (by taking $k = \ell - n$).

We concluded $\mathit{even}(m - n)$.

The proof pattern for implication

You wish to prove $P_1 \Rightarrow P_2$

Proof pattern.

assert the **premise** P_1

(then derive/infer)

... logical/mathematical consequences ...

(until you can)

assert the **conclusion** P_2

With all this you have proven $P_1 \Rightarrow P_2$.

A proof with cases I

Recall the statement

> If $p = r \cdot s$ and p is prime, then one of r and s equals 1 and the other one equals p.

Logical structure:

$$(p = r \cdot s) \wedge prime(p) \;\Rightarrow\; (r = 1 \wedge s = p) \vee (s = 1 \wedge r = p).$$

What did we do to prove this one? To begin with, we have an implication.

We assumed the premise $(p = r \cdot s) \wedge prime(p)$

Then, $r \mid p$

Then, since p is prime, $r = 1$ or $r = p$.

Then, we proceeded in **two cases**.

A proof with cases II

Because $r = 1$ or $r = p$ we can continue in two cases.

In the first case we assume $r = 1$.

Therefore $p = 1 \cdot s$.

And thus $s = p$.

Hence, $(r = 1 \land s = p) \lor (s = 1 \land r = p)$.

In the second case we assume $r = p$.

Therefore $p = p \cdot s$.

And thus $1 = s$.

Hence, $(r = 1 \land s = p) \lor (s = 1 \land r = p)$.

In both cases we have concluded $(r = 1 \land s = p) \lor (s = 1 \land r = p)$.

The by-cases proof pattern

Assuming $P_1 \lor P_2$ you wish to prove P_3.

Proof pattern.

assert $P_1 \lor P_2$

Case 1. assert P_1.

... logical/mathematical consequences ...

assert P_3

Case 2. assert P_2.

... logical/mathematical consequences ...

assert P_3

Since in both cases we obtained P_3, we have proved it assuming $P_1 \lor P_2$.

Some observations about by-cases

1. It generalizes easily to more than two cases. If we start from a disjunction of k statements, then we will have k cases.

2. The cases need not be *mutually exclusive*, as they were (almost) in our example: $(r = 1) \vee (r = p)$. We will give examples later in the course.

3. The disjunction that yields the cases need not appear as part of the assumptions in the original statement. In fact $(r = 1) \vee (r = p)$ did not. You can see a more striking example in another segment in this module.