#1 On Proofs

#1.1 Implication and *Modus Ponens*

Modus ponens is the elimination of implication. It's the starting point of all logics. It goes like this:

1. I assume P implies Q (written $P \Rightarrow Q$).
2. I show P is true.
3. Therefore Q is true.

Here I say "elimination of implication" because we begin with the assumption that $P \Rightarrow Q$ and *eliminate* it to just Q. The *introduction* of implication would look like this.

1. I assume P.
2. I show from P that Q is true.
3. Therefore $P \Rightarrow Q$.

Most basic proofs take one of these two forms. You are usually trying to establish either (i) that something is true by consequence of a known, true implication, or (ii) that an implication is true. The latter is called a *theorem* or *lemma*; the former is an application of a theorem. I find it helpful to think this way: we introduce and eliminate implications.

#1.2 Proof by Construction: Unfolding Definitions

Recall first the definition of "even" and "odd".

Definition 1. *Let $n \in \mathbb{Z}$. We say that n is* even *if there exists $k \in \mathbb{Z}$ such that $n = 2k$. We say n is* odd *otherwise.*

Note that, by consequence of the *division algorithm* (number theory / discrete math), we know n is equivalently odd if there exists k such that $n = 2k + 1$.

Now, for a proof by *unfolding definitions.*

Claim 1. *The sum of an even and odd number is odd.*

Question: What form of implication are we using here? Are we introducing or eliminating an implication? What is the implication?

Proof. Let $n, m \in \mathbb{Z}$ such that n is even and m is odd. What's next? Unfold definitions to see that there exists $k, q \in \mathbb{Z}$ s.t:

$$n = 2k \tag{1}$$
$$m = 2q + 1 \tag{2}$$

It follows that

$$\begin{aligned} &n + m \\ =&2k + (2q + 1) \\ =&2(k + q) + 1. \end{aligned}$$

As $n + m$ can be written in the form $2(k + q) + 1$, it is odd by definition. $\square$

#1.3 Proof by Construction (Existence)

Existential claims rely on showing the existence of an element that exhibits some property. Existential claims are a bit of their own proof style because you often have to *construct* a single answer. For example:

Claim 2. *There exists $n \in \mathbb{N}$ that is equal to the sum of its* proper divisors*. (Here* proper *means not equal to n itself.)*

Proof. $1 + 2 + 3 = 6$. ☐

#1.4 Proof by Counter-Example

How about this one.

Claim 3. *If n is prime, then $2^n - 1$ is prime.*

Consider

$$2^{11} - 1 = 2047 = 23 * 89$$

#1.5 Proof by Cases / Exhaustion

My first thesis to you is that computation is a *concept* with many theoretical interpretations. If I'm permitted a second thesis, it's this: induction is not as hard as you believe it to be. You can think of induction as a proof by cases where you get an extra hypothesis to work with. (Fundamentally, that is what it is.)

Let's consider a proof by cases without the inductive hypothesis.

Definition 2 (Boolean)**.** *A* Boolean *variable b is either the value T or F. In other words, it has **only** these two cases.*

Claim 4 (Boolean Double Negation)**.** *For any Boolean variable x, we have $\neg\neg b = b$.*

Proof. Proceed by cases.

Case (True). Suppose $b = T$. Then

$$\begin{aligned} & b \\ = & \neg(\neg T) \\ = & \neg F \\ = & T \\ = & b \end{aligned}$$

Case (False). Supose $b = F$.

$$\begin{aligned} & b \\ = & \neg(\neg F) \\ = & \neg T \\ = & F \\ = & b \end{aligned}$$

☐

Note here we are not really establishing an implication beyond the hypothesis that b is a Boolean. It depends on your particular logical philosophy if this is a conditional.

#1.6 Proof By Induction

A proof by induction is a proof by cases in which we get an *inductive hypothesis* on one or more of our cases. You are most familiar I am sure with induction as something performed on the naturals (either with or without 0). This is in fact a specific case of what's called *structural induction*—meaning proof over any *inductive structure*. Strings and trees, for example, are inductive structures. We will get to those later in the semester and stick to the naturals, for now. An example:

Claim 5. *For all $n \in \mathbb{N}$, the sum of $1 \ldots n$ equals $\frac{n(n+1)}{2}$.*

$$\sum_{1}^{n} = \frac{n(n+1)}{2}$$

Proof. Proceed by case analysis (induction).

Case $(n = 1)$. For $n = 1$, we have

$$\sum_{1}^{1} = 1 = \frac{2}{2} = \frac{1(1+1)}{2} = \frac{n(n+1)}{2}$$

and so the claim holds.

Case $(n > 1)$. Here we do the tricky bit. Suppose the claim is true for all $n - 1$, that is:

$$\sum_{1}^{n-1} = \frac{(n-1)(n+1-1)}{2} = \frac{n(n-1)}{2}$$

This is our hypothesis: we get to assume it for free. Now we try to prove the claim is true for one greater than $n - 1$—that is, n. Observe that

$$\sum_{1}^{n} = \sum_{1}^{n-1} + n$$

and invoke the inductive hypothesis:

$$\sum_{1}^{n} = \frac{n(n-1)}{2} + n$$

Now let's do the math together to get the result we want.

$$\begin{aligned}
&\frac{n(n-1)}{2} + n \\
&= \frac{n(n-1)}{2} + \frac{2n}{2} \\
&= \frac{2n + n(n-1)}{2} \\
&= \frac{2n + n^2 - n}{2} \\
&= \frac{n^2 + n}{2} \\
&= \frac{n(n+1)}{2}
\end{aligned}$$

$\square$

I know that induction challenges everyone. I encourage you to *always* try the following.

1. Identify the base case. What is the claim for the base case?
2. *Write out the inductive hypothesis explicitly.* State it! So you know that the IH is *an assumption* that you get to use.
3. What is the claim for the step case?
4. How might the inductive hypothesis help you prove the step case?

#1.7 Proof by Contradiction / Non-Constructive Proof

Finally, we get to everyone's favorite bit: proof by contradiction. Proof by contradiction is what's known as a *non-constructive proof* because it allows you to prove the existence of solutions without actually stating what they are.

Formally, a proof by contradiction has the form:

1. Assume $\neg A$.
2. Show that $\neg A$ implies false—in other words, it's impossible that A is false.
3. Therefore A.

This works because of what's called the *law of excluded middle (LEM)*, which states that, for all propositions A it is always true that:

$$A \vee \neg A$$

In other words, no matter the A, either the left or right operand must be true. So, a proof by contradiction shows that $\neg A$ (the right) is not true, therefore we may conclude A (the left). Note that the other direction—to assume A (i.e., the left), show A is false, therefore A is false (i.e., conclude the right)—is *not* a proof by contradiction. But such a distinction is not terribly necessary to keep in mind right now. I just share it because logicians are pedantic and I don't want them to yell at me.

Let's consider a trickier example. This is also an example of "proof by cases". Recall first the following definition.

Definition 3 (Rational Numbers)**.** *A number $n \in \mathbb{R}$ is rational if there exists $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ such that $n = \frac{p}{q}$. The set of rational numbers is denoted $\mathbb{Q}$, which is a proper subset of $\mathbb{R}$.*

Claim 6. *the square root of 2 is irrational.*

Proof. We presume that all real numbers are either rational or irrational. In other words, the following is true:

$$\sqrt{2} \in \mathbb{Q} \vee \sqrt{2} \notin \mathbb{Q}$$

Question: Do you see how this is an invocation of the law of excluded middle?

Now, proceed by case analysis.

Case ($\sqrt{2} \notin \mathbb{Q}$). We are done! The claim is to show exactly this.

Case ($\sqrt{2} \in \mathbb{Q}$). Suppose $\sqrt{2} \in \mathbb{Q}$. By definition, there must be p and q such that $\sqrt{2} = \frac{p}{q}$. In particular, presume that p and q are *mutually prime*: they have no factors in common. (If they did, we can just factor those out.) It follows that

$$\begin{aligned}
\sqrt{2} &= \frac{p}{q} \\
\Rightarrow 2 &= \frac{p^2}{q^2} \\
\Rightarrow 2q^2 &= p^2
\end{aligned}$$

In other words, we have shown that p^2 is even—it has 2 as a divisor. It is important to now see that if p^2 is even, so is p. I won't prove this, but think about it—you can't multiply an odd number by itself and get an even number. Since p is necessarily even, let's unfold the definition: there must exist k such that $p = 2k$. Now, substitute in for the above.

$$\begin{aligned}
&2q^2 = p^2 \\
=&2q^2 = (2k)^2 \\
=&2q^2 = 4k^2 \\
=&q^2 = 2k^2
\end{aligned}$$

And so q^2 is even! By the argument above, so is q.

Question: How do we conclude the proof, now? Where is the contradiction?

We have contradicted our assumption that p and q have no mutual factors. If both are even, they share a factor of 2. We cannot thus make the assumption that $\sqrt{2}$ is rational without also assuming a contradiction. Thus it must be the case (as per the LEM) that $\sqrt{2}$ is irrational. $\square$

Question: Why is this non-constructive? Or, a better way to put it: Tell me what the square root of 2 is.