Proofs

People tend to find proofs scary and hard, but really they are not as scary as they seem. In fact, a great deal of proofs can be achieved by just following steps carefully and diligently, being sure to make your working clear.

The purpose of this note is to demystify proofs and hopefully make them less intimidating by providing structured frameworks to do them in.

It will cover:
- logical reasoning proofs
  - these are a great primers and way to practice proof techniques
- Proof by induction
  - the most common type of proof that I have done
  - a beautiful proving structure that allows you to focus on the meat of the proof alone, lowering your cognitive load by breaking the proof into manageable cases
- some general tips
- Proof by contradiction
  - for absolute statements including words like "all" or "none"
  - an important tool to have in your arsenal
  - unfortunately, diligence and structure can't quite take you the whole way here...

Logical Reasoning

Now, you could use truth tables, but these quickly become tedious with big terms. Utalising logical axioms is another option, but we want to teach you a principled way of proving logical formula without having to assume such things - yes those rules Abed assumed! Also some of your old friends may not even feature in the logic we're teaching. I'm looking at you LEM!

So how do we want you to do it?

Here is my recipe:

1. Assume anything before an implication

2. Solve, remembering: but details
                              details

   - to unpack AND's
   - case on OR's
   - proof by contradiction is your friend (when you have LEM)
   - you can conclude anything from false.

Then present them-wise, (I like to number my lines so I can list them as enabling for a step.

Best to see it in action:

$$\neg A \Rightarrow A \Rightarrow B$$

1. ASS ¬A   ] step 1   nice to justify
2. ASS A   all steps
3. ⊥
4. B   (1) + (2)
             derive anything from ⊥   ] step 2

Induction

When it comes to showing that something is the case for all types defined by rules, we always reach for our favourite tool: induction!

Proof by induction recipe:

1. Decide who to induct on.
   - this can only be a premise
   - Generally, it is the most "relevant" premise
   - When you have a choice between two of the same type, pick the one with the most interesting rule in what you are trying to prove
   - Don't get too hung up on this choice, you can always change your mind if it doesn't work out

2. Take the proof case by case; one case per rule
   - remember to assume your premises
   - write down the IH if it is a recursive rule

If you are stuck, write all the facts you knew in front of you, and consider in turn if any can help.

Abstract thoughts:

I see proof by induction as similar to foldr: you are taking a step back and working at a higher level of abstraction so that you can just focus on the interesting parts of the proof.

With foldr, the problem of crushing a

list is seperated into two concerns: the traversal and management of the list, and then how the list is crushed. Foldr manages the former for you, allowing you to focus on the latter. Foldr to provide as the base case and given the crushed list so far, and the next elem of the list how you should make the new result that encorporates this new element.

Proof by induction is similar: it seperates out the logic of how proving for each creation rule will prove it for every value of that type. Instead of arguing:

$$\frac{\qquad}{} \text{EMPTY}$$
$$\vdots$$
$$\frac{\qquad}{oc:ocs} \text{CONS}$$

"since we have proved it for cons and empty any list has the structure that it is same number of CONS followed by empty thus we have proved it for all lists"

We can just say:
"Proof by induction on lists"

And break into the cons and empty cases, and use the induction hypothesis as a vessel for the above argument

General Advice

REMINDER: Proofs are hard.

Don't worry too much about them. All we want from you is to have a go. Best thing to do is timebox them so you don't waste time banging your head against the sheet. Your time IS would be better spent understanding the solutions when they come out.

If stuck in a proof :

- Make sure you have broken into cases if its by induction
- Do the easier cases first
- Write down all the facts you know that are related to what you are trying to prove e.g. induction hypothesis or the rules
- Take a break.
- Set a timer - if you still have no idea by the time it goes off, just leave it, we will give you feedback on what you have done and you should ensure you understand the solution when it comes.

Moral = if you don't know what to do:
  - write your goal
  - list your assumptions
  - hope you then see how to glue them together

Contradiction

This is mostly as often it requires some divine inspiration.

Luckily, there are some steps you can take even without such inspiration.

Whenever a proof statement uses a word like "all" or "no" ie something must hold universally, this should make you think proof by contradiction cos all you need is one example that breaks.

This is where the divine inspiration comes in. Worry not tho, there can only be a couple of Q's in an exam that require true ingenuity because of the way marks scale (60% of marks must be course basics, then only the last 10% can be truely hard so the super smart kids can shine off). Also by the time of the exam you will have seen a few proofs by contradictions and know the usual suspects.