How to Write a Proof

Intro

When it comes to proof questions, many of you know how to carry out the relevant computations (once you know what the relevant computations are), but are unsure about:

(i) How these computations fit into a "proof";

(ii) How to figure out which are the relevant computations to do, when given a proof question.

The purpose of this note is to guide you on how to write a proof, and remind you of the various kinds of proof questions you've encountered thus far in the course.

What is a Proof?

In mathematics, there are things that we know to be true and there are things we don't (yet) know. A proof is a way of using the information that we know or assume to be true, in order to deduce something that we don't yet know to be true:

How to Write a Proof?

You need to communicate to the examiner that you understand what you need to prove, what information you are allowed to assume to be true and how to carry out the relevant computations to deduce what you want to show to be true.

Many of you get stuck or are intimidated by proof questions. This is often just a psychological barrier, which can be overcome by breaking up the question into more manageable components. One way to do this is to follow the three steps below whenever you are faced with a proof question:

- **Step 1:** *Write down what you need to prove*
  - E.g. "We want to prove that ...."
- **Step 2:** *Write down the relevant information from the question, and what we are allowed to assume to be true*
  - E.g. "We know that K is a field…", "We assume that a is non-zero"… etc.
- **Step 3:** *Use the relevant information from our lecture notes to manipulate the information in Step 2 to compute the desired result stated in Step 1.*
  - This "relevant information" may include (but is not limited to):
    - Important definitions and properties (e.g. positive definiteness of inner product)
    - Axioms of semi-rings, rings, fields…

- Theorems (e.g. Theorem 1 from Handout 1)
- Formulas (e.g. how to reflect a point across a line)

> Rule of Thumb: If the question mentions that we are operating in a **field**, and we are interested in some **non-zero element** $a \neq 0$ in the field, you probably have to use the fact that a has a **multiplicative inverse** somehow, i.e. there exists some a^{-1} such that $a^{-1} \times a = 1$

Examples of Proofs:

1) Prove a statement is true, given a particular assumption

In mathematics, many statements are true only under special hypotheses or assumptions. One way of expressing this logical relationship is to say that A implies B, or in logical notation:

$$A \Rightarrow B$$

where the symbol "⇒" means "implies". In plain words, this means that "If A is true, then B is true."

Remark: Note that if A implies B, and B implies C, then A implies C. In logical notation, if $A \Rightarrow B$ and $B \Rightarrow C$, then $A \Rightarrow C$, i.e. if A is true, then C is true.

Many proof questions are of this flavour – they will ask you to prove a statement (i.e. "B") under specific hypotheses (i.e. "A"). In which case, following the three steps template, your answer should look something like:

- **Step 1:** *Write down what you need to prove*
  - In this case: "We want to prove B"
- **Step 2:** *Write down relevant info/assumptions from the question:*
  - In this case: "We assume that A is true."
- **Step 3:** *Use relevant knowledge to manipulate info from Step 2 to get to Step 1*
  - In this case, our answer may look something like:
    - "Because of Reason X, we know that $A \Rightarrow A'$. Since A is (assumed to be) true, this means that A' is also true.
    - Because of Reason Y, we know that $A' \Rightarrow B$. Since we just showed that A' to be true, we know that B is also true.
    - Since this is exactly what we wanted to prove (see Step 1), we are done with the proof!"

2) Proof by Induction

We are familiar with the idea of a function $f(x)$ – it takes a number "x" as input, and spits out another number "$f(x)$" as output. We also know what that x is a variable – i.e. as far as the function $f(x)$ is concerned, x is not just one particular value but rather a whole range of values.

A similar idea is going on when we talk about induction. However, here we are dealing with *statements* $P(n)$ rather than *functions* – $P(n)$ takes a number "n" as input, and spits out a mathematical statement about n , i.e. "$P(n)$", which may or may not be true.

The ***classical*** induction problem[1] looks something like this: we want to prove that the statement $P(n)$ is true for all natural numbers n. But how do we actually prove this?

One option is to manually compute that $P(0)$ is true, $P(1)$ is true, $P(2)$ is true… but there are infinitely many numbers for us to check, so it is impossible for us to manually verify that $P(n)$ is true for all natural numbers n. So this option doesn't work. What should we do now?

"Proof by induction" gives us the answer to our prayers by using the strategy of "Prove a statement is true, given a particular assumption" in a very clever way.

Recall our previous remark that if A implies B, and B implies C, then A implies C. Note that we can iterate this sort of reasoning indefinitely:

- If $A \Rightarrow B$ and $B \Rightarrow C$, then $A \Rightarrow C$.
  - *In particular, if A is true, then C is also true.*
- If $A \Rightarrow B$, $B \Rightarrow C$, and $C \Rightarrow D$, then $A \Rightarrow D$.
  - *In particular, if A is true, then D is also true.*
- If $A \Rightarrow B$, $B \Rightarrow C$, $C \Rightarrow D$ and $D \Rightarrow E$, then $A \Rightarrow E$
  - *In particular, if A is true, then E is also true.*

  … etc.

Applying this observation to our problem of proving $P(n)$ is true for all n, we have the following:

- If $P(0) \Rightarrow P(1)$ and $P(1) \Rightarrow P(2)$, then $P(0) \Rightarrow P(2)$
  - *In particular, if* $P(0)$ *is true, then* $P(2)$ *is also true.*

- If $P(0) \Rightarrow P(1)$, $P(1) \Rightarrow P(2)$ and $P(2) \Rightarrow P(3)$, then $P(0) \Rightarrow P(3)$
  - *In particular, if* $P(0)$ *is true, then* $P(3)$ *is also true.*

- If $P(0) \Rightarrow P(1)$, $P(1) \Rightarrow P(2)$, $P(2) \Rightarrow P(3)$, and $P(3) \Rightarrow P(4)$, then $P(0) \Rightarrow P(4)$
  - *In particular, if* $P(0)$ *is true, then* $P(4)$ *is also true.*

  … etc.

[1] IMPORTANT: There are variations of this set-up – see Exercise 1 for examples of this!

Once you've convinced yourself of the above line of reasoning, it should be clear to you why proof by induction requires us to check the following two things:

- **Base Case:** $P(0)$ is true
- **Inductive step:** $P(n) \Rightarrow P(n+1)$

In particular, note that:

(i) Proving the inductive step means that we know that $P(0) \Rightarrow P(1)$, $P(1) \Rightarrow P(2)$, $P(2) \Rightarrow P(3)$ etc.;

(ii) Proving that $P(0)$ is true proves that $P(1), P(2), P(3)$ etc. are also true (once we proved the inductive step)

Exercise 1.1 (b)

QUESTION: Prove by induction that $2^n < n!$ for all natural numbers greater than 3.

(*Note: I'm being a little pedantic and including more detail in my answer here than is probably required during the exam – I'm just writing out my thought process in case people are still confused by how to do proof by induction questions…*)

- **Step 1:** *Write down what you need to prove*
  - *Remark:*
    - *When doing proof by induction, we need to be clear what our $P(n)$ is.*
  - *In this case:*
    - Define $P(n)$: $2^n < n!$
    - We want to prove by induction $P(n)$ is true for all natural numbers greater than 3

- **Step 2:** *Write down relevant info/assumptions from the question:*
  - *In this case:*
    - We only need to prove $P(n)$ is true for all natural numbers greater than 3.
    - Hence, for this question, our base case is $P(4)$.[2]

- **Step 3:** *Use relevant knowledge to manipulate info from Step 2 to get to Step 1*
  - *Proof by induction requires us to check two things:*

  - **1. Base Case:** $P(4)$ is true

    To show $P(4)$ is true, we need to show that: $2^4 < 4!$

    To show this, we compute:

[2] Since we aren't interested in $P(0), P(1), P(2)$ and $P(3)$

- $2^4 = 16$
- $4! = 24$

And we observe that:

$$16 < 24$$

Which thus shows that (as desired):

$$2^4 < 4!$$

- **2. Inductive Step:** $P(n) \Rightarrow P(n+1)$, for all $n > 3$

  Note that the inductive step is a mini-proof that asks us to prove a mathematical statement given a particular assumption. So let's follow the three steps again:

  - Step 2a: *Write down what you need to prove*.
    - *In this case:*
      - We want to prove $P(n+1)$ is true,
        i.e. $P(n+1)$: $2^{n+1} < (n+1)!$
  - Step 2b: *Write down relevant info/assumptions*
    - *In this case:*
      - We assume that $P(n)$ is true, i.e. $P(n)$: $2^n < n!$
      - We also assume that n>3
  - Step 2c: *Use relevant knowledge to manipulate info to get to Step 2a*
    - *In this case:*
      - First, we observe that
        - $2^{n+1} = 2 * 2^n$
        - $(n+1)! = (n+1) * n!$
      - Hence, proving the following inequality:

        $$2^{n+1} < (n+1)!$$

        is the same as proving the following inequality:

        $$2 * 2^n < (n+1) * n! \text{ ----------(*)}$$

      - Question: How can we use the inequality in $P(n)$ to prove the above inequality?

        Note: if we multiply both sides of $P(n)$ by 2, we get:

        $$2^n < n!$$
        $$\Rightarrow 2 * 2^n < 2 * n! \text{ ----------(**)}$$

        Note further that since n>3 (see Step 2b), this yields:

$3 < n$
$\Rightarrow 2 < n$ (since 2 < 3 < n)
$\Rightarrow 2 < n + 1$
$\Rightarrow 2 * n! < (n + 1) * n!$ ----------(***)

- Putting the two inequalities (**) and (***) together yields:

$2 * 2^n < 2 * n! < (n + 1) * n!$
$\Rightarrow 2 * 2^n < (n + 1) * n!$
$\Rightarrow 2^{n+1} < (n + 1)!$

where the final implication follows from our remarks about $P(n + 1)$ in (*). This proves the inductive step, and we are thus done!

3) Prove something is a loop invariant

See Handout for a detailed solution to Exercise 2.1.

4) Prove a statement is true by splitting it into different cases

One way to solve a complicated problem is to break it up into smaller problems which are more manageable. We then solve all the smaller problems, and argue that this solves the original problem.

See the following question from Exercise Sheet 3:

Exercise 3.2

Prove that in any algebra of vectors (over any field) we have the following implication

$$a \cdot \vec{v} = \vec{0} \quad \Longrightarrow \quad a = 0 \text{ or } \vec{v} = \vec{0}$$

(Hint: Assume $a \cdot \vec{v} = \vec{0}$ and make a case distinction on whether $a = 0$ or not.)

- **Step 1:** *Write down what you need to prove*
  - *In this case:*
    - We want to prove that $a = 0$ or $\vec{v} = \vec{0}$ is true.

- **Step 2:** *Write down relevant info/assumptions from the question:*
  - *In this case:*
    - We assume that $a * \vec{v} = \vec{0}$
    - We are operating in "an algebra of vectors over any field", hence a is an element of a field.

- **Step 3:** *Use relevant knowledge to manipulate info from Step 2 to get to Step 1*
  - Remark: There are only two possibilities for what value a can take – either $a = 0$ or $a \neq 0$. Hence, we can split the problem into two cases.

- **CASE 1:** $a = 0$
  - Note: If $a = 0$, then clearly the statement we want to prove in Step 1 is true (i.e. $a = 0$ or $\vec{v} = \vec{0}$)

- **CASE 2:** $a \neq 0$
  - If $a \neq 0$, then the only way the statement "$a = 0$ or $\vec{v} = \vec{0}$" can still be true is if $\vec{v} = 0$.
  - So what we have to prove in Case 2 is:

$$a \neq 0 \Rightarrow \vec{v} = \vec{0}$$

  - Note: since $a \neq 0$ and a is an element of a field, it has a multiplicative inverse a^{-1} such that $a^{-1} * a = 1$

  - Now, note:

$$\begin{aligned} \vec{v} &= 1 * \vec{v} \\ &= (a^{-1} * a) * \vec{v} && \text{(since } a^{-1} * a = 1\text{)} \\ &= a^{-1} * (a * \vec{v}) && \text{(since multiplication is associative)} \\ &= a^{-1} * \vec{0} \\ &= \vec{0} \end{aligned}$$

  - We have thus computed that indeed $\vec{v} = \vec{0}$, and we are done!

5) Prove the existence of something

Questions like this requires us to use the given information to "cook up" the desired thing we want to prove the existence of. An example is the following question:

Exercise 2.2 (b)

(b) Let $\mathbb{K}$ be a finite field and let a be a non-zero element of $\mathbb{K}$. Prove that for any element b of $\mathbb{K}$ there is an element c in $\mathbb{K}$ such that $a \times c = b$. Conclude that every element of $\mathbb{K}$ occurs in every row of the multiplication table of $\mathbb{K}$ exactly once, except for the row of zero.

- **Step 1:** *Write down what you need to prove*
  - *In this case:*
    - We want to prove that there exists an element c in K such that $a * c = b$ (given some element $a \neq 0$, and any element b of K)

- **Step 2:** *Write down relevant info/assumptions from the question:*
  - *In this case:*
    - K is a finite field.
    - a is a non-zero element of K.

        - In particular, since K is a field and $a \neq 0$, this means it has a multiplicative inverse a^{-1} such that $a^{-1} * a = 1$
    - b is an element of K.

- **<u>Step 3:</u>** *Use relevant knowledge to manipulate info from Step 2 to get to Step 1*

    - So given an element $a \neq 0$, and any element b of K, how can we cook up this element c such that $a * c = b$?

    - One possibility is to define c as $c = a^{-1} * b$.

    - A quick computation verifies that this is indeed the correct choice since:

      $$a * c = a * (a^{-1} * b) = (a^{-1} * a) * b = 1 * b = b$$

      Which is exactly what we wanted.

      To recap: what have we done? We were given an element $a \neq 0$, and *any* element b of K. Based only on this information, we managed to cook up a c such that $a * c = b$, as desired!