Proof-writing Workshop

What is a good proof, and how do we write one?
Our Game Plan

1. [The majority of our time will be spent here] Walk linearly through our proof virtues from our website. We’ll provide you with many “foolproof” tips for how to achieve each virtue and examples/non-examples!

2. Talk about the process of developing a proof

3. Quickly introduce our friend WLOG, a technique to make your proofs more efficient
“A good proof makes all members of the CS22 community understand why the claim is true.”
Approximate what your reader will be like

- Just like writing an essay, one of the most important skills needed when writing a proof is *approximating* how your reader will receive your words.

- **A good heuristic:** your proofs, *when read aloud*, should make sense to an arbitrary member of the CS22 community.
Be kind to your reader

- Avoid words like “clearly”, “obviously”, “trivially”, “simply”
- What’s easy for you to see may not generalize to others
- Your job is to make what you’re seeing easy for others to see, not to state that it is
Statements should be grounded in concepts, vocabulary, and notation that the CS22 community understands.
Cite results, don’t just use them

- **Remind** your reader of any relevant items that they have recently learned in class or from a previous homework, or things they should know but might have forgotten [1]

- Don’t just say...
  
  Therefore, *blah blah blah*.”

- Instead, say...
  
  “Therefore, by [REALLY COOL RESULT HERE], *blah blah blah*."

Two examples

- If the concept of a rational number was only recently learned in class...
  - **Remind your reader:** “Recall that a rational number can be expressed as a fraction.”
  - **Before saying:** “Since x is rational, we can set x = m/n, where m and n are natural numbers, and n is greater than 0.” \[2\]

- **Don’t just say...**
  - Because (a, b) and (b, c) are in R, so must (a, c).

- **Instead say...**
  - Because (a, b) and (b, c) are in R, by the transitivity of R, so must (a, c).
The do’s and don’ts of notation

- If you have an object in your proof that you are going to refer back to many times, it deserves a name!
- Names are like abbreviations; they package information efficiently

  - Consider an arbitrary member of the codomain. Let us find a member of the domain the our function maps to this arbitrary member of the codomain. Take the arbitrary member of the codomain and add in the fixed element we chose during our map description to it.
  - How could we make this better?
The do’s and don’ts of notation

- Be careful about reusing variable names.
  - Consider an arbitrary non-empty set, $S$.
  - Consider an arbitrary integer, $x$, such that $x < |S|$.
  - $S = \{x \in P(S) \mid |x| < x\}$
  - $S = S \times S$
- What’s wrong here? How could we make this better?
The do’s and don’ts of notation

- Be careful about mixing symbols and words.
  - Don’t replace a single word with a single symbol, just like you wouldn’t write “3 + four”.
  - Similarly, don’t write “We know $\exists$ a bijection...”. Be consistent within a given context.
The do’s and don’ts of notation

- Miscellaneous tips
  - **Instead of**...
    - Let the n elements of S be a, b, c...
    - Let the n elements of S be a_1, a_2, \ldots, a_n
  - Sets get *uppercase* names (E.g. Let S be a set)
  - Elements get *lowercase* name
    (E.g. Let x be an arbitrary element of S)
**Vocabulary**: Let vs. Suppose

Let
Let $S$ be a set with $n$ elements.
Let $R$ be a relation on $S$.

Suppose
Suppose $n$ is even.
Suppose $R$ is transitive.
Arguments need to be **sound**: that is, foundational statements need to be true, and jumps in the argument need to be justified and logical.
Turn & Talk: Warm Up

Turn to your neighbor and explain the steps of making peanut butter and jelly sandwich, and suppose your neighbor were a 3-year old child.

What needed to be explained? What didn’t? How did the fact that your neighbor is 3 years old affect your explanation?
Small steps, not leaps

- Start from what the community knows
- Intermediate steps
  - Explain jumps from A to B
  - An arbitrary community member should be able to answer the question *of how you got from A to B* without much mental labor
Turn & Talk: How can our proof be improved?

- **Claim**: If an equivalence relation $R$ on $A$ is antisymmetric, $R$ is the identity relation. [The identity relation is $\{(x, x) \mid x \text{ in } A\}$.]

- **Proof**:  
  If $(a, b)$ is in $R$ where $a \neq b$, then $(b, a)$ must be in $R$. So $R$ must be the identity relation.
Proofs should minimize mental labor from their audience. This involves...
Organization: Break your proof into digestible chunks for the reader.
Turn & Talk: How can we improve this?

We want to show that $A \cap B = (A \cup B) \setminus (A^c \cup B^c)$ through the set element method. To show that $A \cap B \subseteq (A \cup B) \setminus (A^c \cup B^c)$, take some arbitrary $x$ in $U$’s space that is also in $A \cap B$. That means $x$ is in both $A$ and $B$, so it must be in $A \cup B$. Also, $x \notin A^c$ and $x \notin B^c$, so $x \notin A^c \cup B^c$, so $x \notin A^c \cup B^c$, so it doesn’t get subtracted from $(A \cup B) \setminus (A^c \cup B^c)$. So $x$ is still in that set, which means $A \cap B \subseteq (A \cup B) \setminus (A^c \cup B^c)$. Now to show that $(A \cup B) \setminus (A^c \cup B^c) \subseteq A \cap B$. Say $x$ is now in $(A \cup B) \setminus (A^c \cup B^c)$. This means it’s in $A \cup B$ but not $A^c \cup B^c$. So if it’s in neither $A^c$ nor $B^c$, then it must be in $A$ and $B$. So, $x \in A \cap B$, and so the two sets are equal by the set element method.
One way of doing this...

We want to show that $A \cap B = (A \cup B) \setminus (A^c \cup B^c)$ through the set element method.

**LHS \subseteq RHS.** First, take some arbitrary $x$ in $U$’s space that is also in $A \cap B$. So we can conclude:

$$x \in A \quad x \notin A^c$$

$$x \in B \quad x \notin B^c$$

Therefore, $x \notin A^c \cup B^c$, so it doesn’t get subtracted from the set minus operation on $(A \cup B)$. So $x$ is still in the RHS, which means $A \cap B \subseteq (A \cup B) \setminus (A^c \cup B^c)$.

**RHS \subseteq LHS.** Next, say $x$ is now in $(A \cup B) \setminus (A^c \cup B^c)$. This means that:

$$x \notin A^c \cup B^c$$

So if it’s in neither $A^c$ nor $B^c$, then it must be in $A \cap B$. So, $(A \cup B) \setminus (A^c \cup B^c) \subseteq (A \cap B)$.

With these two claims established, we can conclude that $A \cap B = (A \cup B) \setminus (A^c \cup B^c)$. 
Organization

- Separate ideas get separate spaces. Use paragraphs!
- Separate and label your **cases**
- Break up sub-proofs into sections (e.g. surjection and injection)
- Break up your calculations!
  - Multiple lines
  - Avoid long lines of math in-text
Coherence: The big picture should be clear to the reader.
Big Picture Coherence

Proofs have **goals** and **structures** (like game plans) for achieving those goals. These should be clear to both you and the reader.

- State goal & game plan.
- Start with what you know.
- Implement game plan.
- End with the desired statement.
"Signposting: It should always be clear to the reader from the proof where the author is in the big picture."
Signposting

$$(x - 2)^2 + (x - 1)^2 = 5^2 \quad 5^2 = 25$$
$$(x - 2)^2 = x^2 - 4x + 4 + x^2 - 2x + 1 = 25$$
$$2x^2 - 6x - 20$$
$$2(x + 2)(x - 5) \quad x = -2, 5 \quad x > 0 \quad x = 5$$

Is it clear what the writer is trying to show here? Does this make you understand why something is true?
Probably not
Signposting

- A good proof should *guide* the reader.
- Don’t just do; **explain why you’re doing what you’re doing**.
- “To prove that $f$ is an equivalence relation, we must show...”
Transition Words

Use transition words to relate your thoughts. Your proof should *flow/have momentum*

- In order to show, We want to show, ...
- Therefore, hence, thus...
- But, although, ....
- That is, In other words, ...
- As needed
Example: Show if $4$ divides $n \in \mathbb{Z}$, then $n$ is even.

- $4$ divides $n$, $n = 4k$ for some integer $k$. $n = 2(2k)$, $n$ is even.

- **How can we make this better?**
Example improved

Example: Show if 4 divides $n \in \mathbb{Z}$, then $n$ is even.

- 4 divides $n$, $n = 4k$ for some integer $k$. $n = 2(2k)$, $n$ is even.
- **How can we make this better?**

Since 4 divides $n$, we have $n = 4k$ for some integer $k$. Thus, $n = 2(2k)$, and we have that $n$ is even, as needed.
Be invitational: invite readers to join our thought process [4]

Write in the present tense.
Use “we” instead of “I”.
Use gentle commands/reminders.

- We will now show that R is transitive.
- Recall that the definition of transitivity states...
Striking a balance between concision and thoroughness: Be concise but thorough, and be thorough but not verbose.
Balance: Symbols and English

- Notation can help make things more concise

- However, staying in *purely* notation - i.e. not using complete English sentences to accompany it - does not convey *understanding* to our readers

- Ultimately hurts efficiency!
Balance: Thoroughness and Concision

- Being thorough ≠ Being wordy
- Omit unnecessary details (this often happens when we’re revising!)
- Multiple perspectives can be good, but redundancy isn’t
Turn & Talk: Example

- n is odd. In other words, n is not even. That is, n cannot be written as $2k$, where $k$ is an integer. That is, n can be written as $2p + 1$, for some integer $p$.

- **How can we make this better?**
Providing motivation:
Examples and diagrams should often be provided to motivate your argument.
Providing Motivation

- You want to give insight into your *thought process*

- Providing examples sometimes does this
  - Note: examples alone are not proofs!

- Using diagrams is often *really helpful* in doing this
Turn & Talk: Example

- We claim equivalence classes do not overlap; that is, two equivalence classes are either entirely equal or completely different.

- How could we use a diagram to our advantage here?
Proof Process
From start to finish!
Where to start?

1. Understand the problem statement: Determine your goal.
2. Development: *Write down* thoughts to develop new ones. Search for possible *game plans.*
A Party Problem

At any party of 1000 people, there are always two people at the party who have the same number of friends at the party.

From: https://jeremykun.com/2011/06/23/the-party-problem/
Understand the problem statement

- Walkthrough and define the terms within the statement.
- Determine your **goal, what it is you want to show.**
- Maybe work through an example to understand what the problem is claiming.
- Be suspicious!
  - Question your assumptions!
  - Try to find counterexamples; the reason they fail can illuminate why something is true.
For the sake of this problem, one cannot be friends with oneself, and friendship is symmetric.
Is this possible with 2 people? 3 people?
Development Step 1: Writing is a versatile tool

START WRITING WHAT YOU KNOW DOWN THAT IS RELATED TO YOUR GOAL. TRY TO MAKE YOUR THOUGHTS CLEAR TO YOURSELF.

Writing is not just a tool for recording thoughts; it is a tool for making them more precise and developing more.
Step 2: Questions to ask yourself

What problems have you seen like this before? Generalize your approach!

What proof tools do you have? What mathematical objects and operations do you have under your belt? How can you mix and match them to achieve your goal?

- Contradiction
- Bijection
- Set-element method
- Direct Proof
- ...and so much more!
Proofread and clean

- **Insert** missing intermediate steps: can a member of the community answer the question “why?” for every step you’ve taken?
- **Eliminate** redundancy.
- Don’t keep red herrings; get rid of the facts you didn’t end up using!
Practice!

Good proof-writing comes with lots of practice.

- Write proofs with friends!
- Write proofs by yourself and then see what your friends think!

“Mathematics is not a spectator sport.”
ASIDE: WLOG

Without loss of generality
What is without loss of generality?

- Helpful when you have arbitrary objects related to each other in some way that you want to name!
- If you know two arbitrary sets A and B are not equal, then you can say...

**WLOG, x is in A, but not in B.**

...*without having to consider if x is in B but not in A!***
Other examples

If time permits
**Improve**: Prove that adding 6 to any integer preserves its parity.

We can express an odd number in the form $2x+1$, where $x$ is an integer. Therefore, if $n$ is an odd number, we can say that $n = 2x + 1$. Let $n$ be an odd number. Then $n = 2x + 1$, and if we add 6 to $n$, we get $2x + 7 = (2x+6) + 1 = 2(x+3) + 1 = 2k + 1$, where $k$ is an integer. Because we can express this number in the form $2k+1$, it is an odd number. We can also express an even number in the form $2x$ where $x$ is an integer. Let $m$ be an even number that we can write as $2x$. When we add 6 to $m$, we get $2x+6$. Pulling a 2 out of the sum we have $2(x+3)$. If we let $p = x+3$, we can say that this becomes $2p$. Because we can express this number in the form $2p$, it is an odd number. We have now shown that in both cases, adding 6 to a number preserves its parity.
Works Referenced

Guidelines for good mathematical writing ([1], [2], [3], [4])
https://www.math.hmc.edu/~su/math131/good-math-writing.pdf

How to write proofs: a quick guide
https://cheng.staff.shef.ac.uk/proofguide/proofguide.pdf

Fool-proof Proofwriting
(CS22 previous year’s workshop!)