Goals of a Proof

Proofs serve two purposes:

- Writing a proof can help ensure that something you believe is actually true (a proof is a way of checking your work).
- A proof is a used to convince someone else that your claim is true (and, in the best case, explain why it’s true).

Finding a proof is an act of creative problem solving, requiring inspiration.

Writing and organizing a proof is mostly “perspiration.”

Writing Proofs

Writing a proof to convince someone else is not just a mathematical challenge, it is also a writing challenge.

Writing a readable, understandable proof is a difficult writing challenge on many levels:

- Notation
- Organization
- Language

Key writing guideline: *Explain what you are doing before you do it.*

- “The proof is by contradiction.”
- “We consider three cases.”
- “We prove the contrapositive.”

Often, a proof or subproof will start with a sketch of the overall plan of the proof, followed by the detailed proof.

Proving Something for Yourself

Theoretical computer science is basically mathematics, so writing proofs is a way of life.

But proofs are often helpful in day-to-day programming, in tricky situations.

When proving something for yourself, the goal is to check your work, so you don’t do things that are wrong or waste a lot of time building on false beliefs.

Advice:

- Adopt a skeptical attitude
  - Ask: “If there were a problem, where would it be?”
  - Watch for standard pitfalls and fallacies.
  - Check whether proof uses everything it ought to use (worry if it’s too easy!)
  - Could the same technique be used to prove something that isn’t true?
- Write it down well enough that you can decipher it a few months or years later.
- Coming up with the right theorems and definitions is an iterative process.
What is a Legitimate Proof Step?

This may be the hardest question to answer.

- Too little detail – the reader gets stuck.
- Too much detail – the reader gets bored, and loses the important stuff in all the triviality.

Here are some guidelines.

- A proof step should be believable by the reader.
- Your reader should, with some effort, be able to fill in the details himself or herself.
- You should know that it would be possible to prove the step formally (with sufficient effort).
- If the previous conditions are not satisfied, you don't have a proof.

Subproofs

Proofs often contain subproofs. Care must be taken to indicate when subproofs begin and end (English is not great for this).

Typically, a subproof will be indicated by as a mini-theorem inside the large proof:

```
First, we prove by contradiction that n must be odd: Suppose it were even. Then ... which contradicts ... Hence, n must be odd.

( rest of proof )
```

or

```
claim: n is odd. We prove this by contradiction ...

( rest of proof )
```

What is “obvious”?

What is obvious? “Intuitively obvious” means “I couldn’t immediately think of a counterexample.”

(My mental translation: “Intuitively obvious” means “Probably wrong.”)

“Obvious” means: “I know this is true, and I know that with sufficient effort I could prove it formally.”
Proof by Cases

1. Explain that you are doing a case analysis.
2. Show that a set of cases is exhaustive.
3. Show that the desired conclusion holds for each case.
4. Hence, the conclusion holds.

Proof by Contradiction

- Explain that you are proving by contradiction.
- Assume the complement of the conclusion.
- Prove that a contradiction results.
- Point out that this proves the desired conclusion.

Proving Implication

- State that you are going to prove $P \rightarrow Q$.
- Assume $P$ (“Suppose $P$ holds . . .”)
- Prove $Q$ follows
- Conclude that $P \rightarrow Q$ holds.

Common Proof Strategies
Proving Biconditionals

This happens so often that several proof styles and strategies have emerged for it.

- State that you are proving $P \iff Q$ (“We prove that $P$ iff $Q$."
- Explain that you are going to prove $P \rightarrow Q$, then assume $P$ and prove $Q$.
- Explain that you are going to prove $Q \rightarrow P$, then assume $Q$ and prove $P$.
- Conclude that you have proved $P \iff Q$.

Often, the two parts of the proof are marked with $\rightarrow$ and $\iff$ (or $\equiv$ and $\iff$).

An alternative is to prove $P \rightarrow Q$ and $\neg P \rightarrow \neg Q$ (the contrapositive of $Q \rightarrow P$).

Also, there is nothing magical about the order of $P$ and $Q$, so the subparts may be proved in a different order, or the converse and inverse may be used.

Proving Transitive Relations

A relation $R$ is transitive if

$\forall x \forall y \forall z (xRy \land yRz) \rightarrow (xRz)$

Many relations that occur in proofs are transitive, including $=, \leftrightarrow, \rightarrow, \leq, <, \geq, >, \subseteq, \supseteq,$ etc.

Here is a style of writing proofs that is very readable, when you can use it. To show $a_1 R a_n$

$\begin{array}{ccc}
\text{Justification} 1 \\
\text{Justification 2} \\
\vdots \\
\text{Justification $n-1$} \\
\end{array}$

Example: $\forall x \exists y (P(x) \lor Q(y)) \iff \forall y \exists x (P(x) \lor Q(y))$

$\begin{array}{ccc}
\neg (P \rightarrow Q) & \iff & \neg (\neg P \lor Q) & \rightarrow \lor \text{Identity} \\
& \iff & (\neg P \land \neg Q) & \rightarrow \text{DeMorgan} \\
& \iff & (P \land \neg Q) & \rightarrow \text{elimination} \\
\end{array}$
Summary

A proof is a convincing argument to a mathematically knowledgeable reader that a claim is true.

- Assume the reader knows basic mathematics and proof rules.
- The proof should be much easier to read than to write (and proofs are almost never easy to read!) An unreadable but “technically correct” proof is almost worthless.
- If you skip details, the reader should be able to fill them in easily.
- A step is obvious if it is both intuitively clear and you know it would be possible to write a formal proof.
- You must learn to use your judgement to write a proof that (you feel) will be clear to the reader.