More English Proofs

CSE 311 Fall 23
Lecture 8

About Grades

Grades were critical in your lives up until now.

If you were in high school, they're critical for getting into college.

If you were at UW or CC applying to CSE, they were key to that application

Regardless of where you're going next, what you **learn** in this course matters FAR more than what your grade is in this course.

If you're planning on industry – interviews matter more than grades.

If you're planning on grad school – letters matter most, those are based on doing work outside of class building off what you learned in class.

About Grades

What that means:

The TAs and I are going to prioritize your learning over debating whether -2 or -1 is " more fair"

If you're worried about "have I explained enough" – write more!

It'll take you longer to write the Ed question than write the extended answer. We don't take off for too much work.

And the extra writing is going to help you learn more anyway.

Regrades

TAs make mistakes!

When I was a TA, I made errors on 1 or 2% of my grading that needed to be corrected. If we made a mistake, file a regrade request on gradescope.

But those are only for mistakes, not for whether "-1 would be more fair"

If you are confused, please talk to us!

My favorite office hours questions are "can we talk about the best way to do something on the homework we just got back?"

If **after** you do a regrade request on gradescope, you still think a grading was incorrect, send email to Robbie.

Regrade requests will close about 1 week after homework is returned.

Integer

We need a basic starting point to be able to prove things.

Objects to work with.

An integer: is any real number with no fractional part.

Some **definitions** to analyze

Even

`Even(x)` := An integer, x, is even if and only if there is an integer k such that $x = 2k$.

Odd

`Odd(x)` := An integer, x, is odd if and only if there is an integer k such that $x = 2k + 1$.

A word on definitions

Definitions are fundamental. Our goal is to communicate precisely.

When you come across an edge case, a definition is the way to solve it.

Is -4 even? Well $\exists k(-4 = 2k)$ (take $k = -2$), so yes it is!

We go to the definition. Not your gut feeling about what feels right.

How do we know something is true? Usually we verify the definition!

A word on definitions

How do we know something is true? Usually we verify the definition!

In other resources (textbooks, Wikipedia, etc.)

You will see things that look like this:

Definition: An integer, x, is even if $\exists k(x = 2k)$.

Notice it says "if" not "if and only if."

A definition is **always** an if and only if. The word "definition" has both directions in it (both the "if" and the "only if").

I really wish people didn't do this. I wish they explicitly said "if and only if" but some people insist that "definition" implies the "only if" direction. Otherwise they'd call it a "sufficient condition" not a "definition"

Our First Direct Proof

Definitions
$\text{Even}(x) \coloneqq \exists k(x = 2k)$

Prove: "For all integers x, if x is even, then x^2 is even." $\forall x\left(\text{Even}(x) \rightarrow \text{Even}\left(x^2\right)\right)$

Proof: Let x be an arbitrary integer. Suppose that x is even.

By definition of even, $x = 2k$ for some integer k.

Squaring both sides, we see that:

$x^2 = (2k)^2 = 4k^2 = 2 \cdot 2k^2$

Because k is an integer, $2k^2$ is also an integer.

So x^2 is two times an integer.

Which is exactly the definition of even, so x^2 is even.

Since x was an arbitrary integer, we conclude that for all integers x, if x is even then x^2 is also even.

Direct Proof Template

Declare an arbitrary variable for each ∀.

Assume the left side of the implication.

Unroll the predicate definitions.

Manipulate towards the goal.

Reroll definitions into the right side of the implication.

Conclude that you have proved the claim.

Prove: $\forall x \left(\text{Even}(x) \rightarrow \text{Even}(x^2)\right)$

Let x be an arbitrary integer.

Suppose that x is even.

Then by definition of even, there exists some integer k such that $x = 2k$.

Squaring both sides, we see that:

$$x^2 = (2k)^2 = 4k^2 = 2 \cdot 2k^2$$

Because k is an integer, then $2k^2$ is also an integer. So x^2 is two times an integer.

So by definition of even, x^2 is even.

Since x was an arbitrary integer, we can conclude that for all integers x, if x is even then x^2 is even.

Direct Proof Steps

These are the usual steps. We'll see different outlines in the future!!

- Introduction
  - Declare an arbitrary variable for each ∀ quantifier
  - Assume the left side of the implication
- Core of the proof
  - Unroll the predicate definitions
  - Manipulate towards the goal (using creativity, algebra, etc.)
  - Reroll definitions into the right side of the implication
- Conclude that you have proved the claim

Another Direct Proof

Prove: "The product of two odd integers is odd."

What's the claim in logic?

How would we prove this claim?

Another Direct Proof

Definitions
$\mathrm{Odd}(x) \coloneqq \exists k(x = 2k + 1)$

Prove: "The product of two odd integers is odd."

$$\forall x \forall y \Big(\big(\mathrm{Odd}(x) \wedge \mathrm{Odd}(y) \big) \rightarrow \mathrm{Odd}(xy) \Big)$$

Another Direct Proof

Prove: "The product of two odd integers is odd."

What's the claim in logic? $\forall x \forall y \left(\left(\mathrm{Odd}(x) \wedge \mathrm{Odd}(y) \right) \rightarrow \mathrm{Odd}(xy) \right)$

How would we prove this claim?
Direct Proof. In particular, we'll let x, y be arbitrary integers. We'll suppose x, y are odd. We'll show that $x \cdot y$ is odd.

Another Direct Proof

Definitions
$\text{Odd}(x) \coloneqq \exists k(x = 2k + 1)$

Prove: "The product of two odd integers is odd."

$$\forall x \forall y \left(\left(\text{Odd}(x) \wedge \text{Odd}(y) \right) \rightarrow \text{Odd}(xy) \right)$$

Let x and y be arbitrary integers. Suppose that x and y are odd. Then by definition of odd, there exists some integer k such that $x = 2k + 1$, and some integer j such that $y = 2j + 1$.

Then multiplying x and y, we can see that:

$$xy = (2k + 1) \cdot (2j + 1) = 4kj + 2j + 2k + 1 = 2(2kj + j + k) + 1$$

Since k, j are integers, $2kj + j + k$ is an integer. So by definition of odd, xy is odd.
Since x, y were arbitrary, we have shown that the product of two odd integers is odd.

A note on Domain of Discourse

"The product of two odd integers is odd."

Domain: Integers

Translation:

$$\forall x \forall y \left(\left(\mathrm{Odd}(x) \wedge \mathrm{Odd}(y) \right) \rightarrow \mathrm{Odd}(xy) \right)$$

Proof Outline:

Let x and y be arbitrary integers.

Suppose x and y are odd.

Show xy is odd.

Domain: Odd Integers

Translation:

$$\forall x \forall y \left(\mathrm{Odd}(xy) \right)$$

Proof Outline:

Let x and y be arbitrary odd integers.

Show xy is odd.

A note on Translation to Logic

- We first translate the claim to predicate logic because:
  - The translation makes it precise what we are proving
  - The translation hints at the structure of the proof

    e.g. for each ∀, introduce an arbitrary variable
- In practice, computer scientists identify the proof claim and structure without predicate logic translation
- Eventually we'll stop asking you to translate to logic first

Square

Definition:

An integer x is square iff there exists an integer k such that $x = k^2$.

$$\text{Square}(x) \coloneqq \exists k \left(x = k^2\right)$$

Yet Another Direct Proof

Definitions
$\text{Square}(x) \coloneqq \exists k \left(x = k^2\right)$

Prove: The product of two square integers is square.

What's the claim in logic?

$$\forall n \forall m \left(\left(\text{Square}(n) \wedge \text{Square}(m) \right) \rightarrow \text{Square}(nm) \right)$$

Prove this claim.

Yet Another Direct Proof

Definitions
$\text{Square}(x) \coloneqq \exists k \left(x = k^2\right)$

Prove: "The product of two square integers is square."

$$\forall n \forall m \left(\left(\text{Square}(n) \wedge \text{Square}(m)\right) \rightarrow \text{Square}(nm)\right)$$

Yet Another Direct Proof

Definitions
$\text{Square}(x) \coloneqq \exists k \left(x = k^2\right)$

Prove: "The product of two square integers is square."

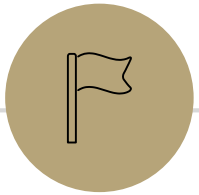
$$\forall n \forall m \left(\left(\text{Square}(n) \wedge \text{Square}(m)\right) \rightarrow \text{Square}(nm)\right)$$

Let n and m be arbitrary integers. Suppose that n and m are square. Then by definition of square, $n = k^2$ for some integer k, and $m = j^2$ for some integer j.

Then multiplying n and m, we can see:

$nm = k^2 \cdot j^2 = (kj)^2$

Since k and j are integers, kj is an integer. So by definition of square, nm is square. Since n and m were arbitrary, we have shown that the product of two square integers is square.



Inference Proofs

A Brief Return to Training Wheels

For about 1.5 lectures, we're going to study "inference proofs"

The rules for these proofs are

1. Strict enough that computers can check them (there are languages designed to do that!)
2. More general than the simplification rules we've seen so far.
   You'll still use the simplification rules!
   But you'll find we can prove more things (at least without significant difficulty).
3. More similar to the proofs we spend most of the quarter writing.

A Brief Return to Training Wheels

The claims and proofs are quite abstract!

Why spend time here?

Some computer scientists use the fully formal (computer-checkable) version of the rules.

Our PL group here contains experts in these topics!

We want your takeaways to be

In principle, any proof we write in this class could be made fully formal and checked.

But it can be a lot of work, so we usually think and communicate in English. We're people after all!

Inference Proofs

A new way of thinking of proofs:

Here's one way to get an iron-clad guarantee:

1. Write down all the facts we know.
2. Combine the things we know to derive new facts.
3. Continue until what we want to show is a fact.

Drawing Conclusions

You know "If it is raining, then I have my umbrella"

And "It is raining"

You should conclude…. I have my umbrella!

For whatever you conclude, convert the statement to propositional logic – will your statement hold for any propositions, or is it specific to raining and umbrellas?

I know $(p \rightarrow q)$ and p, I can conclude q

Or said another way: $[(p \rightarrow q) \wedge p] \rightarrow q$

Modus Ponens

The inference from the last slide is always valid. I.e.

$$[(p \rightarrow q) \wedge p] \rightarrow q$$

Has only True rows in its truth table (it's a tautology)

Modus Ponens – a formal proof

$[(p \to q) \wedge p] \to q$	
$\equiv [(\neg p \vee q) \wedge p] \to q$	Law of Implication
$\equiv [p \wedge (\neg p \vee q)] \to q$	Commutativity
$\equiv [(p \wedge \neg p) \vee (p \wedge q)] \to q$	Distributivity
$\equiv [\mathrm{F} \vee (p \wedge q)] \to q$	Negation
$\equiv [(p \wedge q) \vee \mathrm{F}] \to q$	Commutativity
$\equiv [(p \wedge q)] \to q$	Identity
$\equiv [\neg(p \wedge q)] \vee q$	Law of Implication
$\equiv [\neg p \vee \neg q] \vee q$	DeMorgan's Law
$\equiv \neg p \vee [\neg q \vee q]$	Associativity
$\equiv \neg p \vee [q \vee \neg q]$	Commutativity
$\equiv \neg p \vee \mathrm{T}$	Negation
$\equiv \mathrm{T}$	Domination

Modus Ponens

The inference from the last slide is always valid. I.e.

$$[(p \rightarrow q) \wedge p] \rightarrow q \equiv \mathrm{T}$$

We use that inference A LOT

So often people gave it a name ("Modus Ponens")

So often…we don't have time to repeat that 12 line proof EVERY TIME.

Let's make this another law we can apply in a single step.

Just like refactoring a method in code.

Notation – Laws of Inference

We're using the "→ " symbol A LOT.

Too much

Some new notation to make our lives easier.

If we know **both** A and B

$\therefore$ We can conclude any (or all) of C, D

A, B

$\therefore$ C, D

"$\therefore$" means "therefore" – I knew A, B therefore I can conclude C, D.

$p \to q, p$

$\therefore$ q

Modus Ponens, i.e. $[(p \to q) \wedge p] \to q)$, in our new notation.

Another Proof

Let's keep going.

I know "If it is raining then I have my umbrella" and "I do not have my umbrella"

I can conclude… It is not raining!

What's the general form? $[(p \rightarrow q) \wedge \neg q] \rightarrow \neg p$

How do you think the proof will go?

If you had to convince a friend of this claim in English, how would you do it?

A proof!

We know $p \to q$ and $\neg q$; we want to conclude $\neg p$.
Let's try to prove it. Our goal is to list facts until our goal becomes a fact.
We'll number our facts, and put a justification for each new one.

A proof!

We know $p \to q$ and $\neg q$; we want to conclude $\neg p$.
Let's try to prove it. Our goal is to list facts until our goal becomes a fact.
We'll number our facts, and put a justification for each new one.

1.	$p \to q$	Given
2.	$\neg q$	Given
3.	$\neg q \to \neg p$	Contrapositive of 1.
4.	$\neg p$	Modus Ponens on 3,2.

Try it yourselves

Suppose you know $p \rightarrow q, \neg s \rightarrow \neg q$,and p.
Give an argument to conclude s.

Pollev.com/robbie

Help me adjust my explanation!

Try it yourselves

Suppose you know $p \to q, \neg s \to \neg q$,and p.
Give an argument to conclude s.

1. $p \to q$	Given
2. $\neg s \to \neg q$	Given
3. p	Given
4. q	Modus Ponens 1,3
5. $q \to s$	Contrapositive of 2
6. s	Modus Ponens 5,4

That was abstract!

Imagine that instead someone had said:

If `next` is `null`, then we go down the else-branch

If the input list is non-empty, then we don't go down the else-branch.

This test uses a non-empty list as input.

Can you conclude anything?

So…why do the abstract proof?

Mostly to practice…

Though sometimes it's helpful to make things abstract.

The more general you make a claim…

The more abstract it is, and therefore more difficult to understand on the surface…

But the more different contexts it can be used in.

More Inference Rules

We need a couple more inference rules.

These rules set us up to get facts in exactly the right form to apply the really useful rules.

A lot like commutativity and associativity in the propositional logic rules.

Eliminate ∧

$$\frac{A \wedge B}{\therefore \quad A, B}$$

$$\frac{\text{I know the fact } A \wedge B}{\therefore \text{ I can conclude } A \text{ is a fact and } B \text{ is a fact } \textbf{separately}.}$$

More Inference Rules

In total, we have two for ∧ and two for ∨, one to create the connector, and one to remove it.

Eliminate ∧

$$\frac{A \wedge B}{\therefore \quad A, B}$$

Intro ∧

$$\frac{A, B}{\therefore \quad A \wedge B}$$

Eliminate ∨

$$\frac{A \vee B, \neg A}{\therefore \quad B}$$

Intro ∨

$$\frac{A}{\therefore A \vee B, B \vee A}$$

None of these rules are surprising, but they are useful.