Quantifier Proofs, English Proofs

CSE 311 Spring 22
Lecture 8

The Direct Proof Rule

$$\frac{\text{Write a proof "given } A \text{ conclude } B\text{"}}{A \to B}$$

$$\boxed{\text{Direct Proof rule}}\quad \frac{A \Rightarrow B}{A \to B}$$

This rule is different from the others – $A \Rightarrow B$ is not a "single fact."
It's an observation that we've done a proof. (i.e. that we showed fact B starting from A.)

We will get a lot of mileage out of this rule…starting today!

Given: $((p \to q) \wedge (q \to r))$
Show: $(p \to r)$

Here's an incorrect proof.

1.	$(p \to q) \wedge (q \to r)$	Given
2.	$p \to q$	Eliminate $\wedge$ (1)
3.	$q \to r$	Eliminate $\wedge$ (1)
4.	p	Given???
5.	q	Modus Ponens 4,2
6.	r	Modus Ponens 5,3
7.	$p \to r$	Direct Proof Rule

Given: $((p \to q) \wedge (q \to r))$
Show: $(p \to r)$

Here's an incorrect proof.

Proofs are supposed to be lists of facts.
Some of these "facts" aren't really facts…

1.	$(p \to q) \wedge (q \to r)$	
2.	$p \to q$	
3.	$q \to r$	Eliminate ∧ (1)
4.	p	Given ????
5.	q	Modus Ponens 4,2
6.	r	Modus Ponens 5,3
7.	$p \to r$	Direct Proof Rule

These facts depend on p.
But p isn't known generally.
It was assumed for the purpose of proving $p \to r$.

Given: $((p \to q) \land (q \to r))$
Show: $(p \to r)$

Here's an incorrect proof.

Proofs are supposed to be lists of facts.
Some of these "facts" aren't really facts...

1. $(p \to q) \land (q \to r)$
2. $p \to q$
3. $q \to r$ — Eliminate $\land$ (1)
4. p — Given ????
5. q — Modus Ponens 4,2
6. r — Modus Ponens 5,3
7. $p \to r$ — Direct Proof Rule

These facts depend on p.
But p isn't known generally.
It was assumed for the purpose of proving $p \to r$.

Given: $((p \to q) \wedge (q \to r))$
Show: $(p \to r)$

Here's a corrected version of the proof.

1. $(p \to q) \wedge (q \to r)$ Given
2. $p \to q$ Eliminate ∧ 1
3. $q \to r$ Eliminate ∧ 1
   - 4.1 p Assumption
   - 4.2 q Modus Ponens 4.1,2
   - 4.3 r Modus Ponens 4.2,3
5. $p \to r$ Direct Proof Rule

When introducing an assumption to prove an implication: Indent, and change numbering.

When reached your conclusion, use the Direct Proof Rule to observe the implication is a fact.

The conclusion is an unconditional fact (doesn't depend on p) so it goes back up a level

Try it!

Given: $p \vee q$, $(r \wedge s) \rightarrow \neg q$, r.
Show: $s \rightarrow p$

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

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

Intro ∧
$$\frac{A; B}{\therefore \quad A \wedge B}$$

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

Direct Proof rule
$$\frac{A \Rightarrow B}{A \rightarrow B}$$

Modus Ponens
$$\frac{P \rightarrow Q; P}{\therefore \quad Q}$$

You can still use all the propositional logic equivalences too!

Try it!

Given: $p \vee q$, $(r \wedge s) \rightarrow \neg q$, r.
Show: $s \rightarrow p$

1. $p \vee q$ Given
2. $(r \wedge s) \rightarrow \neg q$ Given
3. r Given
    4.1 s Assumption
    4.2 $r \wedge s$ Intro ∧ (3,4.1)
    4.3 $\neg q$ Modus Ponens (2, 4.2)
    4.4 $q \vee p$ Commutativity (1)
    4.5 p Eliminate ∨ (4.4, 4.3)
5. $s \rightarrow p$ Direct Proof Rule

Inference Rules

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

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

Intro ∧
$$\frac{A; B}{\therefore \quad A \wedge B}$$

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

Direct Proof rule
$$\frac{A \Rightarrow B}{A \rightarrow B}$$

Modus Ponens
$$\frac{P \rightarrow Q; P}{\therefore \quad Q}$$

You can still use all the propositional logic equivalences too!

Inference Proofs in Predicate Logic

Proofs with Quantifiers

We've done symbolic proofs with propositional logic.

To include predicate logic, we'll need some rules about how to use quantifiers.

Eliminate ∀

$$\frac{\forall x\, P(x)}{\therefore P(a) \text{ for any } a}$$

Intro ∃

$$\frac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$$

Intro ∀

$$\frac{P(a);\, a \text{ is arbitrary}}{\therefore \quad \forall x\, P(x)}$$

Eliminate ∃

$$\frac{\exists x P(x)}{\therefore \; P(c) \text{ for a fresh } c}$$

Let's see a good example, then come back to those "arbitrary" and "fresh" conditions.

Proof Using Quantifiers

Suppose we know $\exists x P(x)$ and $\forall y[\ P(y) \rightarrow Q(y)]$. Conclude $\exists x Q(x)$.

Eliminate ∀

$$\frac{\forall x\ P(x)}{\therefore\ P(a) \text{ for any } a}$$

Intro ∃

$$\frac{P(c) \text{ for some } c}{\therefore\quad \exists x\ P(x)}$$

Intro ∀

$$\frac{P(a);\, a \text{ is arbitrary}}{\therefore\quad \forall x\ P(x)}$$

Eliminate ∃

$$\frac{\exists x P(x)}{\therefore\ P(c) \text{ for a fresh } c}$$

Proof Using Quantifiers

Suppose we know $\exists x P(x)$ and $\forall y[\, P(y) \to Q(y)]$. Conclude $\exists x Q(x)$.

Intro $\exists$

$$\frac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$$

Eliminate $\exists$

$$\frac{\exists x P(x)}{\therefore \quad P(c) \text{ for a fresh } c}$$

Eliminate $\forall$

$$\frac{\forall x\, P(x)}{\therefore\, P(a) \text{ for any } a}$$

Intro $\forall$

$$\frac{P(a);\, a \text{ is arbitrary}}{\therefore \quad \forall x\, P(x)}$$

Proof Using Quantifiers

Suppose we know $\exists x P(x)$ and $\forall y[\, P(y) \rightarrow Q(y)]$. Conclude $\exists x Q(x)$.

1. $\exists x P(x)$ Given
2. $P(a)$ Eliminate ∃ 1
3. $\forall y[P(y) \rightarrow Q(y)]$ Given
4. $P(a) \rightarrow Q(a)$ Eliminate ∀ 3
5. $Q(a)$ Modus Ponens 2,4
6. $\exists x Q(x)$ Intro ∃ 5

Intro ∃

$$\frac{P(c) \text{ for some } c}{\therefore\ \exists x\, P(x)}$$

Eliminate ∃

$$\frac{\exists x P(x)}{\therefore\ P(c) \text{ for a fresh } c}$$

Eliminate ∀

$$\frac{\forall x\, P(x)}{\therefore P(a) \text{ for any } a}$$

Intro ∀

$$\frac{P(a);\, a \text{ is arbitrary}}{\therefore\ \forall x\, P(x)}$$

Proofs with Quantifiers

We've done symbolic proofs with propositional logic.

To include predicate logic, we'll need some rules about how to use quantifiers.

Eliminate ∀

$$\frac{\forall x\, P(x)}{\therefore\ P(a) \text{ for any } a}$$

Intro ∃

$$\frac{P(c) \text{ for some } c}{\therefore\ \exists x\, P(x)}$$

Intro ∀

$$\frac{P(a);\, a \text{ is arbitrary}}{\therefore\ \forall x\, P(x)}$$

Eliminate ∃

$$\frac{\exists x P(x)}{\therefore\ P(c) \text{ for a fresh } c}$$

"arbitrary" means a is "just" a variable in our domain.
It doesn't depend on any other variables and wasn't introduced with other information.

Proofs with Quantifiers

We've done symbolic proofs with propositional logic.

To include predicate logic, we'll need some rules about how to use quantifiers.

Eliminate $\forall$

$$\frac{\forall x\, P(x)}{\therefore P(a) \text{ for any } a}$$

Intro $\exists$

$$\frac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$$

Intro $\forall$

$$\frac{P(a);\, a \text{ is arbitrary}}{\therefore \qquad \forall x\, P(x)}$$

Eliminate $\exists$

$$\frac{\exists x P(x)}{\therefore \quad P(c) \text{ for a fresh } c}$$

"fresh" means c is a new symbol (there isn't another c somewhere else in our proof).

Fresh and Arbitrary

Suppose we know $\exists x P(x)$. Can we conclude $\forall x P(x)$?

1. $\exists x\, P(x)$ Given
2. $P(a)$ Eliminate $\exists$ (1)
3. $\forall x\, P(x)$ Intro $\forall$ (2)

This proof is **definitely** wrong.
(take $P(x)$ to be "is a prime number")

a wasn't **arbitrary**. We knew something about it – it's the x that exists to make $P(x)$ true.

Intro $\exists$
$$\frac{P(c) \text{ for some } c}{\therefore\ \exists x\, P(x)}$$

Eliminate $\exists$
$$\frac{\exists x P(x)}{\therefore\ P(c) \text{ for a fresh } c}$$

Eliminate $\forall$
$$\frac{\forall x\, P(x)}{\therefore\ P(a) \text{ for any } a}$$

Intro $\forall$
$$\frac{P(a);\ a \text{ is arbitrary}}{\therefore\ \forall x\, P(x)}$$

Fresh and Arbitrary

Intro ∀

$$\frac{P(a);\ a \text{ is arbitrary}}{\therefore \quad \forall x\, P(x)}$$

Eliminate ∃

$$\frac{\exists x P(x)}{\therefore \quad P(c) \text{ for a fresh } c}$$

You can trust a variable to be **arbitrary** if you introduce it as such.

If you eliminated a ∀ to create a variable, that variable is arbitrary. Otherwise it's not arbitrary – it depends on something.

You can trust a variable to be **fresh** if the variable doesn't appear anywhere else (i.e. just use a new letter)

Fresh and Arbitrary

Eliminate ∀

$$\frac{\forall x\, P(x)}{\therefore P(a) \text{ for any } a}$$

Intro ∃

$$\frac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$$

There are no similar concerns with these two rules.

Want to reuse a variable when you eliminate ∀? Go ahead.

Have a c that depends on many other variables, and want to intro ∃?

Also not a problem.

Arbitrary

In section, you said: $[\exists y \forall x\, P(x, y)] \to [\forall x \exists y\, P(x, y)]$. Let's prove it!!

Arbitrary

In section, you said: $[\exists y \forall x\, P(x,y)] \rightarrow [\forall x \exists y\, P(x,y)]$. Let's prove it!!

1.1 $\exists y \forall x\, P(x,y)$	Assumption
1.2 $\forall x\, P(x,c)$	Elim $\exists$ (1.1)
1.3 Let a be arbitrary.	--
1.4 $P(a,c)$	Elim $\forall$ (1.2)
1.5 $\exists y\, P(a,y)$	Intro $\exists$ (1.4)
1.6 $\forall x \exists y\, P(x,y)$	Intro $\forall$ (1.5)

2. $[\exists y \forall x\, P(x,y)] \rightarrow [\forall x \exists y\, P(x,y)]$ Direct Proof Rule

Arbitrary

In section, you said: $[\exists y \forall x\, P(x,y)] \rightarrow [\forall x \exists y\, P(x,y)]$. Let's prove it!!

1.1 $\exists y \forall x\, P(x,y)$	Assumption
1.2 $\forall x\, P(x,c)$	Elim $\exists$ (1.1)
1.4 $P(a,c)$	Elim $\forall$ (1.2)
1.5 $\exists y\, P(a,y)$	Intro $\exists$ (1.4)
1.6 $\forall x \exists y\, P(x,y)$	Intro $\forall$ (1.5)

2. $[\exists y \forall x\, P(x,y)] \rightarrow [\forall x \exists y\, P(x,y)]$ Direct Proof Rule

It is not required to have "variable is arbitrary" as a step before using it. But many people (including Robbie) find it helpful.

Find The Bug

Let your domain of discourse be integers.
We claim that given $\forall x \exists y$ `Greater`(y, x), we can conclude $\exists y \forall x$ `Greater`(y, x)
Where `Greater`(y, x) means $y > x$

1.	$\forall x \exists y$ `Greater`(y, x)	Given
2.	Let a be an arbitrary integer	--
3.	$\exists y$ `Greater`(y, a)	Elim $\forall$ (1)
4.	`Greater`(b, a)	Elim $\exists$ (2)
5.	$\forall x$ `Greater`(b, x)	Intro $\forall$ (4)
6.	$\exists y \forall x$ `Greater`(y, x)	Intro $\exists$ (5)

Find The Bug

1.	$\forall x \exists y\ \texttt{Greater}(y, x)$	Given
2.	Let a be an arbitrary integer	--
3.	$\exists y\ \texttt{Greater}(y, a)$	Elim ∀ (1)
4.	$\texttt{Greater}(b, a)$	Elim ∃ (2)
5.	$\forall x\ \texttt{Greater}(b, x)$	Intro ∀ (4)
6.	$\exists y \forall x\ \texttt{Greater}(y, x)$	Intro ∃ (5)

b is not a single number! The variable b depends on a. You can't get rid of a while b is still around.
What is b? It's probably something like $a + 1$.

Bug Found

There's one other "hidden" requirement to introduce $\forall$.

"No other variable in the statement can depend on the variable to be generalized"

Think of it like this -- b was probably $a + 1$ in that example.

You wouldn't have generalized from `Greater`$(a + 1, a)$

To $\forall x$ `Greater`$(a + 1, x)$. There's still an a, you'd have replaced all the a's.

x depends on y if y is in a statement when x is introduced.

This issue is much clearer in English proofs, which we'll start next time.

English Proofs

LOSE THE TRAINING WHEELS™

What’s Next

We’re taking off the training wheels!

Our goal with writing symbolic proofs was to prepare us to write proofs in English.

Let’s get started.

The next 3 weeks:

- Practice communicating clear arguments to others.
- Learn new proof techniques.
- Learn fundamental objects (sets, number theory) that will let us talk more easily about computation at the end of the quarter.

Warm-up

Even

An integer x is even if (and only if) there exists an integer z, such that $x = 2z$.

Let your domain of discourse be integers.

Let $\texttt{Even}(x) := \exists y(x = 2y)$.

Prove "if x is even then x^2 is even."

Write a symbolic proof (with the extra rules "Definition of $\texttt{Even}$" and "Algebra").

Then we'll write it in English.

What's the claim in symbolic logic? $\forall x(\texttt{Even}(x) \rightarrow \texttt{Even}(x^2))$

If x is even, then x^2 is even.

1. Let a be arbitrary	
2.1 $\texttt{Even}(a)$	Assumption
2.2 $\exists y\ (2y = a)$	Definition of Even (2.1)
2.3 $2z = a$	Elim $\exists$(2.2)
2.4 $a^2 = 4z^2$	Algebra (2.3)
2.5 $a^2 = 2 \cdot 2z^2$	Alegbra (2.4)
2.6 $\exists w(2w = a^2)$	Intro $\exists$ (2.5)
2.7 $\texttt{Even}(a^2)$	Definition of Even
3. $\texttt{Even}(a) \rightarrow \texttt{Even}(a^2)$	Direct Proof Rule (2.1-2.7)
4. $\forall x(\texttt{Even}(x) \rightarrow \texttt{Even}(x^2))$	Intro $\forall$ (3)

If x is even, then x^2 is even.

1. Let a be arbitrary		Let x be an arbitrary even integer.
2.1 $\texttt{Even}(a)$	Assumption	By definition, there is an integer y such that $2y = x$.
2.2 $\exists y\ (2y = a)$	Definition of Even (2.1)	
2.3 $2z = a$	Elim $\exists$(2.2)	
2.4 $a^2 = 4z^2$	Algebra (2.3)	Squaring both sides, we see that $x^2 = 4y^2 = 2 \cdot 2y^2$.
2.5 $a^2 = 2 \cdot 2z^2$	Alegbra (2.4)	
2.6 $\exists w(2w = a^2)$	Intro $\exists$ (2.5)	Because y is an integer, $2y^2$ is also an integer, and x^2 is two times an integer.
2.7 $\texttt{Even}(a^2)$	Definition of Even	Thus x^2 is even by the definition of even.
3. $\texttt{Even}(a) \rightarrow \texttt{Even}(a^2)$	Direct Proof Rule (2.1-2.7)	
4. $\forall x(\texttt{Even}(x) \rightarrow \texttt{Even}(x^2))$	Intro $\forall$ (3)	Since x was an arbitrary even integer, we can conclude that for every even x, x^2 is also even.

Converting to English

Start by introducing your assumptions.

Introduce variables with “let.” Introduce assumptions with “suppose.”

Always state what type your variable is. English proofs don’t have an established domain of discourse.

Don’t just use “algebra” explain what’s going on.

We don’t explicitly intro/elim $\exists/\forall$ so we end up with fewer “dummy variables”

Let x be an arbitrary even integer.
By definition, there is an integer y such that $2y = x$.

Squaring both sides, we see that $x^2 = 4y^2 = 2 \cdot 2y^2$.

Because y is an integer, $2y^2$ is also an integer, and x^2 is two times an integer.
Thus x^2 is even by the definition of even.
Since x was an arbitrary even integer, we can conclude that for every even x, x^2 is also even.

Why English Proofs?

Those symbolic proofs seemed pretty nice. Computers understand them, and can check them.

So what's up with these English proofs?

They're far easier for **people** to understand.

But instead of a computer checking them, now a human is checking them.