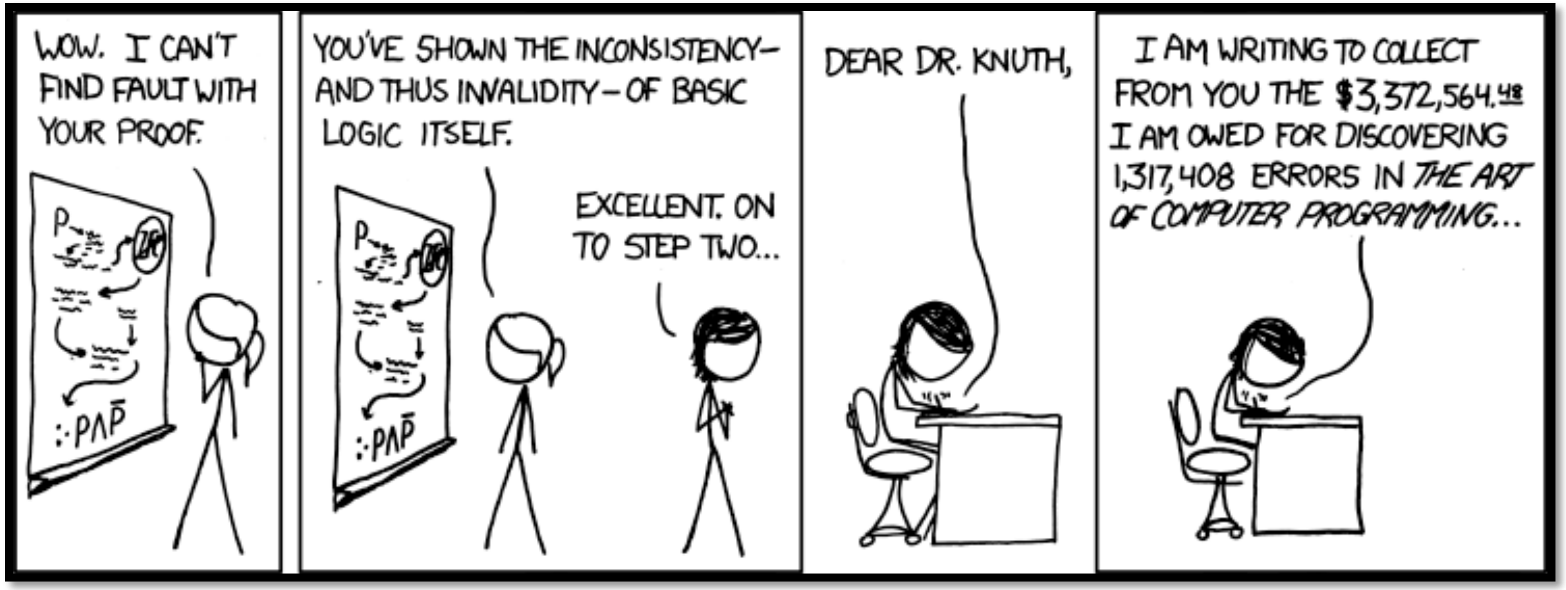

xkcd.com/816/

Quantified Inference Proofs + English Language proofs

Proof Using Quantifiers

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

Eliminate ∀

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

Intro ∃

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

Intro ∀

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

Eliminate ∃

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

Proof Using Quantifiers

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

Intro ∃

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

Eliminate ∃

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

Eliminate ∀

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

Intro ∀

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

Proof Using Quantifiers

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

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

Intro ∃

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

Eliminate ∃

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

Eliminate ∀

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

Intro ∀

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

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 ∀

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

Intro ∃

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

Intro ∀

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

Eliminate ∃

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

"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 ∀

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

Intro ∃

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

Intro ∀

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

Eliminate ∃

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

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

Fresh and Arbitrary

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

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

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

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

Intro $\exists$

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

Eliminate $\exists$

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

Eliminate $\forall$

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

Intro $\forall$

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

Fresh and Arbitrary

Intro ∀

$a(c)$; c is arbitrary

$\therefore \quad \forall x\, a(x)$

Eliminate ∃

$\exists x a(x)$

$\therefore \quad a(c)$ 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 ∀

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

Intro ∃

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

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

Let's prove $[\exists y \forall x\, a(x,y)] \rightarrow [\forall x \exists y\, a(x,y)]$.

Eliminate ∧: $\dfrac{A \wedge B}{\therefore\ A, B}$

Eliminate ∨: $\dfrac{A \vee B, \neg A}{\therefore\ B}$

Intro ∧: $\dfrac{A; B}{\therefore\ A \wedge B}$

Intro ∨: $\dfrac{A}{\therefore\ A \vee B, B \vee A}$

Direct Proof rule: $\dfrac{A \Rightarrow B}{A \rightarrow B}$

Modus Ponens: $\dfrac{P \rightarrow Q; P}{\therefore\ Q}$

You can still use all the propositional logic equivalences too!

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

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

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

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

Excluded Middle: $\dfrac{}{\therefore\ A \vee \neg A}$

DeMorgan's (Quantifiers):

$\neg(\forall x\, A) \equiv \exists x(\neg A)$

$\neg(\exists x A) \equiv \forall x(\neg A)$

Arbitrary

Let's prove $[\exists y \forall x\ a(x,y)] \to [\forall x \exists y\ a(x,y)]$.

1.1 $\exists y \forall x\ a(x,y)$	Assumption
1.2 $\forall x\ a(x,c)$	Elim ∃ (1.1)
1.3 Let z be arbitrary.	--
1.4 $a(z,c)$	Elim ∀ (1.2)
1.5 $\exists y\ a(z,y)$	Intro ∃ (1.4)
1.6 $\forall x \exists y\ a(x,y)$	Intro ∀ (1.5)
2. $[\exists y \forall x\ a(x,y)] \to [\forall x \exists y\ a(x,y)]$	Direct Proof Rule

Find The Bug

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

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.	$b \geq a$	Elim ∃ (2)
5.	$\forall x \texttt{ Greater}(b, x)$	Intro ∀ (4)
6.	$\exists y \forall x \texttt{ Greater}(y, x)$	Intro ∃ (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.	$b \geq a$	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 arbitrary. The variable b depends on a. Even though a is arbitrary, b is not!

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…

LOSE THE TRAINING WHEELS™

English Proofs

Now

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."

We'll go through 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 $a^2 = 2 \cdot 2z^2$	Algebra (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.

Let's do another!

First a definition

Rational

A real number x is rational if (and only if) there exist integers n and m, with $m \neq 0$ such that $x = n/m$.

$$\texttt{Rational}(x) \coloneqq \exists n \exists m(\texttt{Integer}(n) \land \texttt{Integer}(m) \land (x = n/m) \land m \neq 0)$$

Let's do another!

"The product of two rational numbers is rational."

What is this statement in predicate logic?

$\forall x \forall y([\texttt{rational}(x) \land \texttt{rational}(y)] \rightarrow \texttt{rational}(xy))$

Remember unquantified variables in English are implicitly universally quantified.

Doing a Proof

$\forall x \forall y([\texttt{rational}(x) \wedge \texttt{rational}(y)] \rightarrow \texttt{rational}(xy))$

"The product of two rational numbers is rational."

DON'T just jump right in!

Look at the statement, make sure you know:

1. What every word in the statement means.
2. What the statement as a whole means.
3. Where to start.
4. What your target is.

Do we need another example of an English proof?

Now You Try

The sum of two even numbers is even.

Make sure you know:

1. What every word in the statement means.
2. What the statement as a whole means.
3. Where to start.
4. What your target is.

Even

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

Fill out the poll everywhere for Activity Credit!

Go to pollev.com/cse311 and login with your UW identity
Or text cse311 to 22333

1. Write the statement in predicate logic.
2. Write an English proof.
3. If you have lots of extra time, try writing the symbolic proof instead.

Here's What I got.

$\forall x \forall y([\texttt{Even}(x) \land \texttt{Even}(y)] \rightarrow \texttt{Even}(x+y))$

Let x, y be arbitrary integers, and suppose x and y are even.

By the definition of even, $x = 2a, y = 2b$ for some integers a and b.

Summing the equations, $x + y = 2a + 2b = 2(a + b)$.

Since a and b are integers, $a + b$ is an integer, so $x + y$ is even by the definition of even.

Since x, y were arbitrary, we can conclude the sum of two even integers is 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.

Sets

Set

A set is an **unordered** group of **distinct** elements.

We'll always write a set as a list of its elements inside {curly, brackets}.

Variable names are capital letters, with lower-case letters for elements.

$A = \{\text{curly, brackets}\}$

$B = \{0,5,8,10\} = \{5,0,8,10\} = \{0,0,5,8,10\}$

$C = \{0,1,2,3,4, \ldots\}$

Sets

Some more symbols:

$a \in A$ (a is in A or a is an element of A) means a is one of the members of the set.

For $B = \{0,5,8,10\}, \quad 0 \in B$.

$A \subseteq B$ (A is a subset of B) means every element of A is also in B.

For $A = \{1,2\}$, $B = \{1,2,3\}$ $A \subseteq B$

Sets

Be careful about these two operations:

If $A = \{1,2,3,4,5\}$

$\{1\} \subseteq A$, but $\{1\} \notin A$

$\in$ asks: is this item in that box?

$\subseteq$ asks: is everything in this box also in that box?

Try it!

Let $A = \{1,2,3,4,5\}$

$B = \{1,2,5\}$

Is $A \subseteq A$?

Is $B \subseteq A$?

Is $A \subseteq B$?

Is $\{1\} \in A$?

Is $1 \in A$?