CSE 311: Foundations of Computing

Lecture 9: Inference proofs predicate logic and English proofs

…LET'S ASSUME THERE EXISTS SOME FUNCTION F(a,b,c…) WHICH PRODUCES THE CORRECT ANSWER–
HANG ON.
THIS IS GOING TO BE ONE OF THOSE WEIRD, DARK-MAGIC PROOFS, ISN'T IT? I CAN TELL.
WHAT? NO, NO, IT'S A PERFECTLY SENSIBLE CHAIN OF REASONING.
ALL RIGHT…
NOW, LET'S ASSUME THE CORRECT ANSWER WILL EVENTUALLY BE WRITTEN ON THIS BOARD AT THE COORDINATES (x, y). IF WE–
I KNEW IT!

Last class: Inference Rules for Quantifiers

Intro ∃

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

Elim ∀

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

Intro ∀

$$\frac{\text{“}\textbf{Let}\ a\ \textbf{be arbitrary*}\text{”}\ldots P(a)}{\therefore\quad \forall x\, P(x)}$$

* in the domain of P. No other name in P depends on a

Elim ∃

$$\frac{\exists x\, P(x)}{\therefore\ P(c)\ \textbf{for some}\ \textbf{\textit{special}}{**}\ c}$$

** c is a NEW name.
List all dependencies for c.

Last class: Inference Rules for Quantifiers

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

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

$$\text{Intro } \forall \quad \frac{\text{“Let } a \text{ be arbitrary*”} \ldots P(a)}{\therefore \quad \forall x\, P(x)}$$

$$\text{Elim } \exists \quad \frac{\exists x\, P(x)}{\therefore \; P(c) \text{ for some } \textit{special}^{**}\ c}$$

* in the domain of P. No other name in P depends on a

** c is a NEW name.
List all dependencies for c.

Example: Prove $\forall x\, P(x) \to \exists x\, P(x)$

Last class: Inference Rules for Quantifiers

Intro ∃

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

Elim ∀

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

Intro ∀

$$\frac{\text{“Let a be arbitrary*”...P(a)}}{\therefore \quad \forall x\ P(x)}$$

* in the domain of P. No other name in P depends on a

Elim ∃

$$\frac{\exists x\ P(x)}{\therefore \ \text{P(c) for some } \textit{special}\text{** c}}$$

** c is a NEW name.
List all dependencies for c.

Example: Prove ∀x P(x) → ∃x P(x)

1.1.	$\forall x\, P(x)$	Assumption
1.2.		
1.3.		
1.4.	$\exists x\, P(x)$	Intro ∃: 1.3
1.	$\forall x\, P(x) \rightarrow \exists x\, P(x)$	Direct Proof Rule

Last class: Inference Rules for Quantifiers

Intro ∃

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

Elim ∀

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

Intro ∀

$$\frac{\text{“Let } a \text{ be arbitrary* ”} \ldots P(a)}{\therefore \quad \forall x\, P(x)}$$

* in the domain of P. No other name in P depends on a

Elim ∃

$$\frac{\exists x\, P(x)}{\therefore \; P(c) \text{ for some } \textit{special}^{**}\ c}$$

** c is a NEW name. List all dependencies for c.

Example: Prove $\forall x\, P(x) \rightarrow \exists x\, P(x)$

1.1. $\forall x\, P(x)$ Assumption

1.2. Let a be an object.

1.3. $P(a)$ Elim ∀: 1.1

1.4. $\exists x\, P(x)$ Intro ∃: 1.3

1. $\forall x\, P(x) \rightarrow \exists x\, P(x)$ Direct Proof Rule

A Prime Example

Domain of Discourse

Integers

Predicate Definitions

$\text{Even}(x) \equiv \exists y\,(x = 2\cdot y)$

$\text{Odd}(x) \equiv \exists y\,(x = 2\cdot y + 1)$

$\text{Prime}(x) \equiv$ “$x > 1$ and $x \neq a\cdot b$ for
all integers a, b with $1<a<x$”

Prove “There is an even prime number”

A Prime Example

Domain of Discourse

Integers

Predicate Definitions

$\text{Even}(x) \equiv \exists y\,(x = 2\cdot y)$

$\text{Odd}(x) \equiv \exists y\,(x = 2\cdot y + 1)$

$\text{Prime}(x) \equiv$ “$x > 1$ and $x \neq a\cdot b$ for all integers a, b with $1<a<x$”

Prove “There is an even prime number”

Formally: prove $\exists x\,(\text{Even}(x) \wedge \text{Prime}(x))$

1.	$\mathbf{2 = 2\cdot 1}$	**Arithmetic**
2.	$\text{Prime}(\mathbf{2})$*	**Property of integers**

* **Later we will further break down** “Prime” **using quantifiers to prove statements like this**

A Prime Example

Domain of Discourse
Integers

Predicate Definitions
$\mathrm{Even}(x) \equiv \exists y\,(x = 2 \cdot y)$ $\mathrm{Odd}(x) \equiv \exists y\,(x = 2 \cdot y + 1)$ $\mathrm{Prime}(x) \equiv$ “$x > 1$ and $x \neq a \cdot b$ for all integers a, b with $1 < a < x$”

Prove “There is an even prime number”

Formally: prove $\exists x\,(\mathrm{Even}(x) \wedge \mathrm{Prime}(x))$

1.	$\mathbf{2} = \mathbf{2} \cdot \mathbf{1}$	**Arithmetic**
2.	$\mathrm{Prime}(\mathbf{2})$ *	**Property of integers**
3.	$\exists y\,(\mathbf{2} = \mathbf{2} \cdot y)$	**Intro** $\exists$: **1**
4.	$\mathrm{Even}(\mathbf{2})$	**Defn of** Even: **3**
5.	$\mathrm{Even}(\mathbf{2}) \wedge \mathrm{Prime}(\mathbf{2})$	**Intro** $\wedge$: **2, 4**
6.	$\exists x\,(\mathrm{Even}(x) \wedge \mathrm{Prime}(x))$	**Intro** $\exists$: **5**

* **Later we will further break down** “Prime” **using quantifiers to prove statements like this**

Even(x) $\equiv \exists y\ (x=2y)$
Odd(x) $\equiv \exists y\ (x=2y+1)$
Domain: Integers

Even and Odd

Intro ∀ $\dfrac{\text{"Let a be arbitrary*"...}P(a)}{\therefore\ \forall x\, P(x)}$

Elim ∃ $\dfrac{\exists x\, P(x)}{\therefore\ P(c) \text{ for some special** } c}$

Prove: "The square of every even number is even."

Formal proof of: $\forall x\,(\text{Even}(x) \rightarrow \text{Even}(x^2))$

3. $\forall x\,(\text{Even}(x)\rightarrow\text{Even}(x^2))$?

Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

Intro ∀ "**Let** a **be arbitrary***"...P(a)
∴ ∀x P(x)

Elim ∃ ∃x P(x)
∴ P(c) **for some *special*** ** c

Prove: "The square of every even number is even."

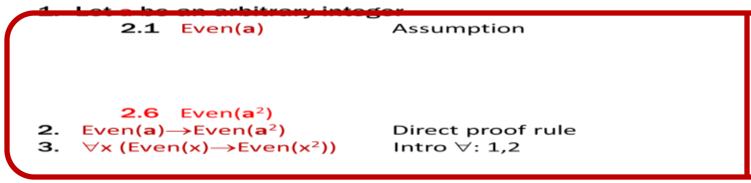
Formal proof of: ∀x (Even(x) → Even(x²))

1. **Let a be an arbitrary integer**

2. Even(**a**)→Even(**a**²) ?
3. ∀x (Even(x)→Even(x²)) Intro ∀: 1,2

Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers



1. Let a be an arbitrary integer
2.1 Even(a) Assumption
2.6 Even(a²)
2. Even(a)→Even(a²) Direct proof rule
3. ∀x (Even(x)→Even(x²)) Intro ∀: 1,2

Elim ∃

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

Prove: "The square of every even number is even."

Formal proof of: $\forall x\, (\text{Even}(x) \rightarrow \text{Even}(x^2))$

1. Let **a** be an arbitrary integer

    2.1 Even(**a**) Assumption

    2.6 Even($\mathbf{a}^2$) ?

2. Even(**a**)→Even($\mathbf{a}^2$) Direct proof rule
3. $\forall x\, (\text{Even}(x) \rightarrow \text{Even}(x^2))$ Intro ∀: 1,2

Even and Odd

Even(x) $\equiv \exists y\ (x=2y)$
Odd(x) $\equiv \exists y\ (x=2y+1)$
Domain: Integers

Intro ∀ $\dfrac{\text{“Let } a \text{ be arbitrary*”} \ldots P(a)}{\therefore \quad \forall x\, P(x)}$

Elim ∃ $\dfrac{\exists x\, P(x)}{\therefore\ P(c) \text{ for some special** } c}$

Prove: “The square of every even number is even.”

Formal proof of: $\forall x\ (\text{Even}(x) \rightarrow \text{Even}(x^2))$

1. Let **a** be an arbitrary integer

2.1 Even(**a**) Assumption

2.2 $\exists y\ (\mathbf{a} = 2y)$ Definition of Even

2.5 $\exists y\ (\mathbf{a}^2 = 2y)$?

2.6 Even($\mathbf{a}^2$) Definition of Even

2. Even(**a**)→Even($\mathbf{a}^2$) Direct proof rule

3. $\forall x\ (\text{Even}(x) \rightarrow \text{Even}(x^2))$ Intro ∀: 1,2

Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

Intro ∀ $\dfrac{\text{“Let } a \text{ be arbitrary*”} \ldots P(a)}{\therefore \quad \forall x\, P(x)}$

Elim ∃ $\dfrac{\exists x\, P(x)}{\therefore P(c) \text{ for some special** } c}$

Prove: “The square of every even number is even.”

Formal proof of: $\forall x\, (\text{Even}(x) \rightarrow \text{Even}(x^2))$

1. Let **a** be an arbitrary integer

2.1	Even(**a**)	Assumption
2.2	∃y (**a** = 2y)	Definition of Even
2.5	∃y ($\mathbf{a}^2$ = 2y)	Intro ∃ rule: ?
2.6	Even($\mathbf{a}^2$)	Definition of Even
2.	Even(**a**)→Even($\mathbf{a}^2$)	Direct proof rule
3.	∀x (Even(x)→Even(x^2))	Intro ∀: 1,2

Need $\mathbf{a}^2 = 2c$
for some **c**

Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

Intro ∀

“Let a be arbitrary*”...P(a)

∴ ∀x P(x)

Elim ∃

∃x P(x)

∴ P(c) for some *special*** c

Prove: “The square of every even number is even.”

Formal proof of: $\forall x\,(\mathrm{Even}(x) \rightarrow \mathrm{Even}(x^2))$

1. Let **a** be an arbitrary integer

2.1	Even(**a**)	Assumption
2.2	∃y (**a** = 2y)	Definition of Even
2.3	**a** = 2**b**	Elim ∃: **b** special depends on **a**
2.5	∃y (**a**^{2} = 2y)	Intro ∃ rule: ?
2.6	Even(**a**^{2})	Definition of Even

Need **a**^{2} = 2c for some **c**

2.	Even(**a**)→Even(**a**^{2})	Direct proof rule
3.	∀x (Even(x)→Even(x^2))	Intro ∀: 1,2

Even and Odd

$\mathrm{Even}(x) \equiv \exists y\ (x=2y)$
$\mathrm{Odd}(x) \equiv \exists y\ (x=2y+1)$
Domain: Integers

Intro ∀ $\dfrac{\text{“Let } a \text{ be arbitrary*”} \ldots P(a)}{\therefore\ \forall x\, P(x)}$

Elim ∃ $\dfrac{\exists x\, P(x)}{\therefore\ P(c) \text{ for some special** } c}$

Prove: “The square of every even number is even.”

Formal proof of: $\forall x\, (\mathrm{Even}(x) \rightarrow \mathrm{Even}(x^2))$

1.	Let a be an arbitrary integer	
2.1	$\mathrm{Even}(a)$	Assumption
2.2	$\exists y\ (a = 2y)$	Definition of Even
2.3	$a = 2b$	Elim ∃: b special depends on a
2.4	$a^2 = 4b^2 = 2(2b^2)$	Algebra
2.5	$\exists y\ (a^2 = 2y)$	Intro ∃ rule
2.6	$\mathrm{Even}(a^2)$	Definition of Even
2.	$\mathrm{Even}(a)\rightarrow\mathrm{Even}(a^2)$	Direct proof rule
3.	$\forall x\ (\mathrm{Even}(x)\rightarrow\mathrm{Even}(x^2))$	Intro ∀: 1,2

Used $a^2 = 2c$ for $c=2b^2$

Why did we need to say that b depends on a?

There are extra conditions on using these rules:

Intro ∀

$$\frac{\text{“Let } a \text{ be arbitrary*”} \ldots P(a)}{\therefore \quad \forall x\, P(x)}$$

* in the domain of P

Elim ∃

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

** c has to be a NEW name.

Over integer domain: $\forall x\, \exists y\, (y \geq x)$ **is True but** $\exists y \forall x\, (y \geq x)$ **is False**

BAD “PROOF”

1.	$\forall x\, \exists y\, (y \geq x)$	Given
2.	**Let a be an arbitrary integer**	
3.	$\exists y\, (y \geq \mathbf{a})$	Elim ∀: **1**
4.	$\mathbf{b} \geq \mathbf{a}$	Elim ∃: **b** special depends on **a**
5.	$\forall x\, (\mathbf{b} \geq x)$	Intro ∀: **2,4**
6.	$\exists y \forall x\, (y \geq x)$	Intro ∃ : **5**

Why did we need to say that b depends on a?

There are extra conditions on using these rules:

Intro ∀ $\dfrac{\text{“Let } a \text{ be arbitrary*”} \ldots P(a)}{\therefore \qquad \forall x\, P(x)}$

* in the domain of P

Elim ∃ $\dfrac{\exists x\, P(x)}{\therefore P(c) \text{ for some } \textit{special}^{**}\ c}$

** c has to be a NEW name.

Over integer domain: $\forall x\, \exists y\, (y \geq x)$ is True but $\exists y \forall x\, (y \geq x)$ is False

BAD “PROOF”

1. $\forall x\, \exists y\, (y \geq x)$ Given
2. Let **a** be an arbitrary integer
3. $\exists y\, (y \geq \mathbf{a})$ Elim ∀: 1
4. $\mathbf{b} \geq \mathbf{a}$ Elim ∃: **b** special depends on **a**
5. $\forall x\, (\mathbf{b} \geq x)$ Intro ∀: 2,4
6. $\exists y \forall x\, (y \geq x)$ Intro ∃ : 5

Can’t get rid of **a** since another name in the same line, **b**, depends on it!

Why did we need to say that b depends on a?

There are extra conditions on using these rules:

Intro ∀

"**Let** a **be arbitrary***"...P(a)

∴ $\forall x\, P(x)$

* in the domain of P. No other name in P depends on a

Elim ∃

$\exists x\, P(x)$

∴ P(c) **for some *special*** c

** c is a NEW name.
List all dependencies for c.

Over integer domain: $\forall x\, \exists y\, (y \geq x)$ **is True but** $\exists y \forall x\, (y \geq x)$ **is False**

BAD "PROOF"

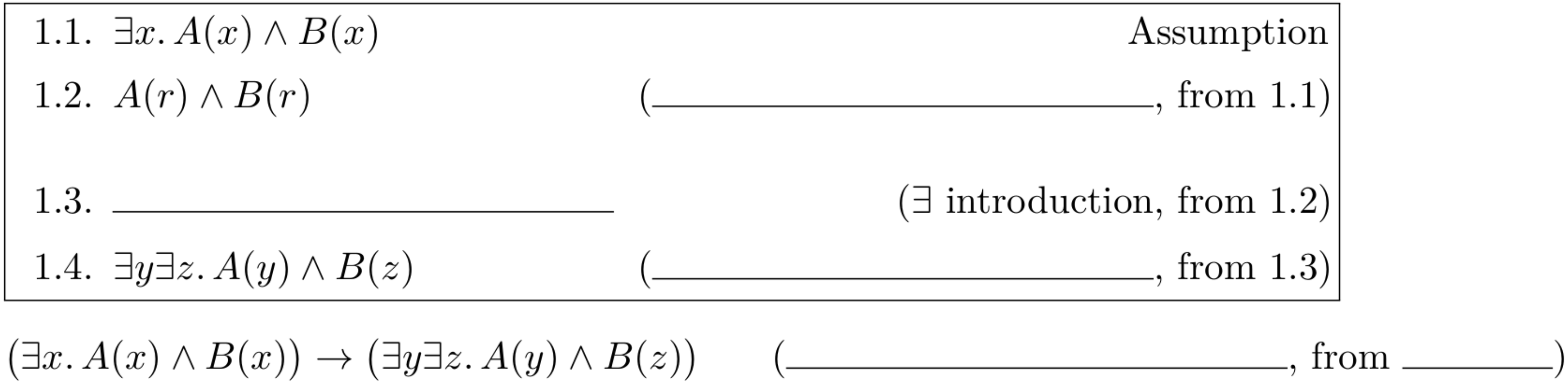
1. $\forall x\, \exists y\, (y \geq x)$ Given
2. Let a be an arbitrary integer
3. $\exists y\, (y \geq a)$ Elim ∀: 1
4. $b \geq a$ Elim ∃: b special depends on a
5. ~~$\forall x\, (b \geq x)$ Intro ∀: 2,4~~
6. $\exists y \forall x\, (y \geq x)$ Intro ∃ : 5

Can't get rid of a since another name in the same line, b, depends on it!

Lecture 9 Activity

You will be assigned to breakout rooms. Please:

- Introduce yourself
- Choose someone to share their screen, showing this PDF
- Fill in the blanks in the following formal proof



1.1. $\exists x.\, A(x) \land B(x)$ Assumption

1.2. $A(r) \land B(r)$ (______________________________, from 1.1)

1.3. ______________________________ ($\exists$ introduction, from 1.2)

1.4. $\exists y \exists z.\, A(y) \land B(z)$ (______________________________, from 1.3)

1. $(\exists x.\, A(x) \land B(x)) \to (\exists y \exists z.\, A(y) \land B(z))$ (______________________________, from __________)

Fill out the poll everywhere for Activity Credit!
Go to pollev.com/philipmg and login with your UW identity

English Proofs

- We often write proofs in English rather than as fully formal proofs
  - They are more natural to read

- English proofs follow the structure of the corresponding formal proofs
  - Formal proof methods help to understand how proofs really work in English…

    … and give clues for how to produce them.

Formal Proofs

- In principle, formal proofs are the standard for what it means to be “proven” in mathematics
  - almost all math (and theory CS) done in Predicate Logic

- But they are **tedious** and impractical
  - e.g., applications of commutativity and associativity
  - Russell & Whitehead’s formal proof that 1+1 = 2 is *several hundred pages* long

    we allowed ourselves to cite “Arithmetic”, “Algebra”, etc.

- Similar situation exists in programming…

Programming

```
%a = add %i, 1
%b = mod %a, %n
%c = add %arr, %b
%d = load %c
%e = add %arr, %i
store %e, %d
```

```
arr[i] = arr[(i+1) % n];
```

Assembly Language

High-level Language

Programming vs Proofs

%a = add %i, 1	Given
%b = mod %a, %n	Given
%c = add %arr, %b	∧ Elim: 1
%d = load %c	Double Negation: 4
%e = add %arr, %i	∨ Elim: 3, 5
store %e, %d	MP: 2, 6
Assembly Language for Programs	**Assembly Language for Proofs**

Proofs

Given

Given

∧ Elim: 1

Double Negation: 4

∨ Elim: 3, 5

MP: 2, 6

what is the “Java” for proofs?

Assembly Language for Proofs

High-level Language for Proofs

Proofs

Given

Given

∧ Elim: 1

Double Negation: 4

∨ Elim: 3, 5

MP: 2, 6

English

Assembly Language for Proofs

High-level Language for Proofs

Proofs

- **Formal proofs follow simple well-defined rules and should be easy for a machine to check**
  - as assembly language is easy for a machine to execute

- **English proofs correspond to those rules but are designed to be easier for humans to read**
  - **also easy to check with practice**

    (almost all actual math and theory CS is done this way)
  - **English proof is correct if the <u>reader</u> believes they could translate it into a formal proof**

    (the reader is the "compiler" for English proofs)

Last class: Even and Odd

$\text{Even}(x) \equiv \exists y\ (x=2y)$
$\text{Odd}(x) \equiv \exists y\ (x=2y+1)$
Domain: Integers

Prove: "The square of every even number is even."

Formal proof of: $\forall x\ (\text{Even}(x) \rightarrow \text{Even}(x^2))$

1.	Let $\mathbf{a}$ be an arbitrary integer	
2.1	$\text{Even}(\mathbf{a})$	Assumption
2.2	$\exists y\ (\mathbf{a} = 2y)$	Definition of Even
2.3	$\mathbf{a} = 2\mathbf{b}$	Elim ∃: **b** special depends on **a**
2.4	$\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$	Algebra
2.5	$\exists y\ (\mathbf{a}^2 = 2y)$	Intro ∃ rule
2.6	$\text{Even}(\mathbf{a}^2)$	Definition of Even
2.	$\text{Even}(\mathbf{a}) \rightarrow \text{Even}(\mathbf{a}^2)$	Direct proof rule
3.	$\forall x\ (\text{Even}(x) \rightarrow \text{Even}(x^2))$	Intro ∀: 1,2

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

English Proof: Even and Odd

Prove "The square of every even integer is even."

Let a be an arbitrary integer.	**1.**	**Let a be an arbitrary integer**	
Suppose a is even.	**2.1**	Even(**a**)	Assumption
Then, by definition, a = 2b for some integer b (dep on a).	**2.2**	∃y (**a** = 2y)	Definition
	2.3	**a** = 2**b**	**b** special depends on **a**
Squaring both sides, we get $a^2 = 4b^2 = 2(2b^2)$.	**2.4**	$a^2 = 4b^2 = 2(2b^2)$	Algebra
So a^2 **is, by definition, even.**	**2.5**	$\exists y\ (a^2 = 2y)$	
	2.6	$\text{Even}(a^2)$	Definition
Since a was arbitrary, we have shown that the square of every even number is even.	**2.**	$\text{Even}(a) \rightarrow \text{Even}(a^2)$	
	3.	$\forall x\ (\text{Even}(x) \rightarrow \text{Even}(x^2))$	

English Proof: Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

Prove "The square of every even integer is even."

Proof: Let **a** be an arbitrary integer. Suppose **a** is even.

Then, by definition, $\mathbf{a} = 2\mathbf{b}$ for some integer b (depending on **a**). Squaring both sides, we get $\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$. So $\mathbf{a}^2$ is, by definition, is even.

Since **a** was arbitrary, we have shown that the square of every even number is even. ■

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y \; (x = 2y)$

Odd(x) ≡ $\exists y \; (x = 2y + 1)$

Domain of Discourse

Integers

Prove "The sum of two odd numbers is even."

Formally, prove $\forall x \, \forall y \, ((\mathrm{Odd}(x) \land \mathrm{Odd}(y)) \rightarrow \mathrm{Even}(x+y))$

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y\ (x = 2y)$

Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse

Integers

Prove "The sum of two odd numbers is even."

Proof: Let x and y be arbitrary integers. Suppose that both are odd.

Then, x = 2a+1 for some integer a (depending on x) and y = 2b+1 for some integer b (depending on x). Their sum is x+y = (2a+1) + (2b+1) = 2a+2b+2 = 2(a+b+1), so x+y is, by definition, even.

Since x and y were arbitrary, the sum of any two odd integers is even. ■

English Proof: Even and Odd

$\mathrm{Even}(x) \equiv \exists y\ (x=2y)$
$\mathrm{Odd}(x) \equiv \exists y\ (x=2y+1)$
Domain: Integers

Prove "The sum of two odd numbers is even."

Let x and y be arbitrary integers.	**1.**	**Let x be an arbitrary integer**	
	2.	**Let y be an arbitrary integer**	
Suppose that both are odd.	**2.1**	$\mathrm{Odd}(\mathbf{x}) \wedge \mathrm{Odd}(\mathbf{y})$	Assumption
	2.2	$\mathrm{Odd}(\mathbf{x})$	Elim ∧: 2.1
	2.3	$\mathrm{Odd}(\mathbf{y})$	Elim ∧: 2.1
Then, x = 2a+1 for some integer a (depending on x) and	**2.4**	$\exists z\ (\mathbf{x} = 2z+1)$	Def of Odd: 2.2
	2.5	$\mathbf{x} = 2\mathbf{a}+1$	Elim ∃: 2.4 (**a** dep **x**)
y = 2b+1 for some integer b (depending on x).	**2.5**	$\exists z\ (\mathbf{y} = 2z+1)$	Def of Odd: 2.3
	2.6	$\mathbf{y} = 2\mathbf{b}+1$	Elim ∃: 2.5 (**b** dep **y**)
Their sum is x+y = … = 2(a+b+1)	**2.4**	$\mathbf{x+y} = \ldots = 2(\mathbf{a+b+1})$	Algebra
so x+y is, by definition, even.	**2.5**	$\exists z\ (\mathbf{x+y} = 2z)$	Intro ∃: 2.4
	2.6	$\mathrm{Odd}(\mathbf{b}^2)$	Def of Even
Since x and y were arbitrary, the sum of any odd integers is even.	**2.**	$\mathrm{Odd}(\mathbf{b}) \rightarrow \mathrm{Odd}(\mathbf{b}^2)$	
	3.	$\forall x\ (\mathrm{Odd}(x) \rightarrow \mathrm{Odd}(x^2))$	

Rational Numbers

Domain of Discourse

Real Numbers

- A real number x is *rational* iff there exist integers p and q with $q \neq 0$ such that $x = p/q$.

$$\text{Rational}(x) \equiv \exists p \, \exists q \; ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge q \neq 0)$$

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) ≡ $\exists p\ \exists q\ ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Formally, prove (Rational(x) ∧ Rational(y))→Rational(x+y)

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) ≡ $\exists p\ \exists q\ ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Proof: Suppose that x and y are rational. Then, x = a/b for some integers a, b, where b≠0, and y = c/d for some integers c,d, where d≠0.

Multiplying, we get that xy = (ac)/(bd). Since b and d are both non-zero, so is bd. Furthermore, ac and bd are integers. By definition, then, xy is rational.

■

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) ≡ $\exists p\ \exists q\ ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Prove: "The product of two rationals is rational."

Proof: Let x and y be arbitrary.

Suppose that x and y are rational. Then, x = a/b for some integers a, b, where b≠0, and y = c/d for some integers c,d, where d≠0.

Multiplying, we get that xy = (ac)/(bd). Since b and d are both non-zero, so is bd. Furthermore, ac and bd are integers. By definition, then, xy is rational.

Since x and y were arbitrary, we have shown that the product of any two rationals is rational. ■

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) $\equiv \exists p\, \exists q\, ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Suppose that x and y are rational.

1.1 $\text{Rational}(x) \wedge \text{Rational}(y)$ **Assumption**

Then, x = a/b for some integers a, b, where b≠0 and y = c/d for some integers c,d, where d≠0.

...

1.4 $\exists p\, \exists q\, ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$
Def Rational: 1.2

1.5 $(x = a/b) \wedge \text{Integer}(a) \wedge \text{Integer}(b) \wedge (b \neq 0)$
Elim ∃: 1.4

1.6 $\exists p\, \exists q\, ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$
Def Rational: 1.3

1.7 $(y = c/d) \wedge \text{Integer}(c) \wedge \text{Integer}(d) \wedge (d \neq 0)$
Elim ∃: 1.4

Rationality

Domain of Discourse

Real Numbers

Predicate Definitions

Rational(x) $\equiv \exists p\ \exists q\ ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Suppose that x and y are rational.

1.1 $\text{Rational}(x) \land \text{Rational}(y)$ **Assumption**

??

Then, x = a/b for some integers a, b, where b≠0 and y = c/d for some integers c,d, where d≠0.

1.4 $\exists p\ \exists q\ ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Def Rational: 1.2

1.5 $(x = a/b) \land \text{Integer}(a) \land \text{Integer}(b) \land (b \neq 0)$

Elim ∃: 1.4

1.6 $\exists p\ \exists q\ ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Def Rational: 1.3

1.7 $(y = c/d) \land \text{Integer}(c) \land \text{Integer}(d) \land (d \neq 0)$

Elim ∃: 1.4

…

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) $\equiv \exists p\, \exists q\, ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Suppose that x and y are rational.

Then, x = a/b for some integers a, b, where b≠0 and y = c/d for some integers c,d, where d≠0.

...

1.1 $\text{Rational}(x) \land \text{Rational}(y)$ **Assumption**

1.2 $\text{Rational}(x)$ **Elim ∧: 1.1**

1.3 $\text{Rational}(y)$ **Elim ∧: 1.1**

1.4 $\exists p\, \exists q\, ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$
Def Rational: 1.2

1.5 $(x = a/b) \land \text{Integer}(a) \land \text{Integer}(b) \land (b \neq 0)$
Elim ∃: 1.4

1.6 $\exists p\, \exists q\, ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$
Def Rational: 1.3

1.7 $(y = c/d) \land \text{Integer}(c) \land \text{Integer}(d) \land (d \neq 0)$
Elim ∃: 1.4

Rationality

Domain of Discourse

Real Numbers

Predicate Definitions

Rational(x) ≡ $\exists p\, \exists q\, ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

...

1.5 $(x = a/b) \wedge \text{Integer}(a) \wedge \text{Integer}(b) \wedge (b \neq 0)$

...

1.7 $(y = c/d) \wedge \text{Integer}(c) \wedge \text{Integer}(d) \wedge (d \neq 0)$

Multiplying, we get xy = (ac)/(bd).

1.10 $xy = (a/b)(c/d) = (ac/bd) = (ac)/(bd)$ **Algebra**

Rationality

Domain of Discourse

Real Numbers

Predicate Definitions

Rational(x) ≡ $\exists p\, \exists q\, ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

…

1.5 $(x = a/b) \land \text{Integer}(a) \land \text{Integer}(b) \land (b \neq 0)$

…

1.7 $(y = c/d) \land \text{Integer}(c) \land \text{Integer}(d) \land (d \neq 0)$

??

Multiplying, we get xy = (ac)/(bd).

1.10 $xy = (a/b)(c/d) = (ac/bd) = (ac)/(bd)$ **Algebra**

Rationality

Domain of Discourse

Real Numbers

Predicate Definitions

Rational(x) ≡ $\exists p\, \exists q\, ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

...

1.5 $(x = a/b) \land \text{Integer}(a) \land \text{Integer}(b) \land (b \neq 0)$

...

1.7 $(y = c/d) \land \text{Integer}(c) \land \text{Integer}(d) \land (d \neq 0)$

1.8 $x = a/b$ **Elim ∧: 1.5**

1.9 $y = c/d$ **Elim ∧: 1.7**

Multiplying, we get xy = (ac)/(bd).

1.10 $xy = (a/b)(c/d) = (ac/bd) = (ac)/(bd)$ **Algebra**

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) ≡ $\exists p\ \exists q\ ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

…

1.5 $(x = a/b) \wedge \text{Integer}(a) \wedge \text{Integer}(b) \wedge (b \neq 0)$

…

1.7 $(y = c/d) \wedge \text{Integer}(c) \wedge \text{Integer}(d) \wedge (d \neq 0)$

…

1.11 $b \neq 0$ **Elim ∧: 1.5***

1.12 $c \neq 0$ **Elim ∧: 1.7**

Since b and d are non-zero, so is bd.

1.13 $bc \neq 0$ **Prop of Integer Mult**

*** Oops, I skipped steps here...**

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions

Rational(x) ≡ $\exists p\ \exists q\ ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

…

1.5 $(x = a/b) \wedge (\text{Integer}(a) \wedge (\text{Integer}(b) \wedge (b \neq 0)))$

…

1.7 $(y = c/d) \wedge (\text{Integer}(c) \wedge (\text{Integer}(d) \wedge (d \neq 0)))$

…

1.11 $\text{Integer}(a) \wedge (\text{Integer}(b) \wedge (b \neq 0)))$ — **Elim ∧: 1.5**

1.12 $\text{Integer}(b) \wedge (b \neq 0)$ — **Elim ∧: 1.11**

1.13 $b \neq 0$ — **Elim ∧: 1.12**

We left out the parentheses...

Rationality

Domain of Discourse

Real Numbers

Predicate Definitions

Rational(x) ≡ $\exists p\ \exists q\ ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

	...	
	1.5 $(x = a/b) \land \text{Integer}(a) \land \text{Integer}(b) \land (b \neq 0)$	
	...	
	1.7 $(y = c/d) \land \text{Integer}(c) \land \text{Integer}(d) \land (d \neq 0)$	
	...	
	1.13 $b \neq 0$	**Elim ∧: 1.5**
	...	
	1.16 $c \neq 0$	**Elim ∧: 1.7**
Since b and d are non-zero, so is bd.	**1.17** $bd \neq 0$	**Prop of Integer Mult**

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) ≡ $\exists p\ \exists q\ ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Furthermore, ac and bd are integers.

…	
1.5 $(x = a/b) \land \text{Integer}(a) \land \text{Integer}(b) \land (b \neq 0)$	
…	
1.7 $(y = c/d) \land \text{Integer}(c) \land \text{Integer}(d) \land (d \neq 0)$	
…	
1.19 $\text{Integer}(a)$	**Elim ∧: 1.5***
…	
1.22 $\text{Integer}(b)$	**Elim ∧: 1.5***
…	
1.24 $\text{Integer}(c)$	**Elim ∧: 1.7***
…	
1.27 $\text{Integer}(d)$	**Elim ∧: 1.7***
1.28 $\text{Integer}(ac)$	**Prop of Integer Mult**
1.29 $\text{Integer}(bd)$	**Prop of Integer Mult**

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) ≡ $\exists p\ \exists q\ ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

…

1.10 $xy = (a/b)(c/d) = (ac/bd) = (ac)/(bd)$

…

1.17 $bd \neq 0$ **Prop of Integer Mult**

…

1.28 $\text{Integer}(ac)$ **Prop of Integer Mult**

1.29 $\text{Integer}(bd)$ **Prop of Integer Mult**

1.30 $\text{Integer}(bd) \land (bc \neq 0)$ **Intro ∧: 1.29, 1.17**

1.31 $\text{Integer}(ac) \land \text{Integer}(bd) \land (bc \neq 0)$

Intro ∧: 1.28, 1.30

1.32 $(xy = (a/b)/(c/d)) \land \text{Integer}(ac) \land \text{Integer}(bd) \land (bc \neq 0)$ **Intro ∧: 1.10, 1.31**

1.33 $\exists p\ \exists q\ ((xy = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Intro ∃: 1.32

1.34 $\text{Rational}(xy)$ **Def of Rational: 1.32**

By definition, then, xy is rational.

Rationality

Domain of Discourse

Real Numbers

Predicate Definitions

Rational(x) ≡ $\exists p\ \exists q\ ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Suppose that x and y are rational.	**1.1** $\text{Rational}(x) \wedge \text{Rational}(y)$	**Assumption**
	…	
	1.10 $xy = (a/b)(c/d) = (ac/bd) = (ac)/(bd)$	
	…	
	1.17 $bd \neq 0$	**Prop of Integer Mult**
	…	
Furthermore, ac and bd are integers.	**1.28** $\text{Integer}(ac)$	**Prop of Integer Mult**
	1.29 $\text{Integer}(bd)$	**Prop of Integer Mult**
	…	
By definition, then, xy is rational.	**1.33** $\text{Rational}(xy)$	**Def of Rational: 1.32**

What's missing?

Rationality

Domain of Discourse

Real Numbers

Predicate Definitions

Rational(x) $\equiv \exists p\, \exists q\, ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Suppose that x and y are rational.

1.1 $\text{Rational}(x) \wedge \text{Rational}(y)$ **Assumption**

...

1.10 $xy = (a/b)(c/d) = (ac/bd) = (ac)/(bd)$

...

1.17 $bc \neq 0$ **Prop of Integer Mult**

...

Furthermore, ac and bd are integers.

1.28 $\text{Integer}(ac)$ **Prop of Integer Mult**

1.29 $\text{Integer}(bd)$ **Prop of Integer Mult**

...

By definition, then, xy is rational.

1.33 $\text{Rational}(xy)$ **Def of Rational: 1.32**

1. $\text{Rational}(x) \wedge \text{Rational}(y) \rightarrow \text{Rational}(xy)$

Direct Proof

Rationality

Domain of Discourse

Real Numbers

Predicate Definitions

Rational(x) $\equiv \exists p\, \exists q\, ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Proof: Suppose that x and y are rational. Then, x = a/b for some integers a, b, where $b \neq 0$, and y = c/d for some integers c,d, where $d \neq 0$.

Multiplying, we get that xy = (ac)/(bd).

Since b and d are both non-zero, so is bd. Furthermore, ac and bd are integers. By definition, then, xy is rational. ■

vs 34 lines of formal proof

English Proofs

- High-level language let us work more quickly
  - should not be necessary to spill out every detail
  - <u>reader</u> checks that the writer is not skipping too much
  - examples so far

    skipping Intro ∧ and Elim ∧

    not stating existence claims (immediately apply Elim ∃ to name the object)

    not stating that the implication has been proven (“Suppose X… Thus, Y.” says it already)
  - (list will grow over time)

- English proof is correct if the <u>reader</u> believes they could translate it into a formal proof
  - the reader is the “compiler” for English proofs

Proof Strategies

Proof Strategies: Counterexamples

To prove $\neg\forall x\ P(x)$, prove $\exists\neg P(x)$:

- Works by de Morgan's Law: $\neg\forall x\ P(x) \equiv \exists x \neg P(x)$
- All we need to do that is find an x where $P(x)$ is **false**
- This example is called a ***counterexample*** to $\forall x\ P(x)$.

e.g. Prove "Not every prime number is odd"

Proof: 2 is prime but not odd, a counterexample to the claim that every prime number is odd. ■

Proof Strategies: Proof by Contrapositive

If we assume $\neg q$ and derive $\neg p$, then we have proven $\neg q \rightarrow \neg p$, which is equivalent to proving $p \rightarrow q$.

1.1.	$\neg q$	Assumption
...		
1.3.	$\neg p$	
1.	$\neg q \rightarrow \neg p$	Direct Proof Rule
2.	$p \rightarrow q$	Contrapositive: 1

Proof Strategies: Proof by Contrapositive

If we assume $\neg$q and derive $\neg$p, then we have proven $\neg$q $\rightarrow$ $\neg$p, which is equivalent to proving p $\rightarrow$ q.

We will prove the contrapositive.

Suppose $\neg q$.

...

Thus, $\neg p$.

1.1.	$\neg q$	Assumption
...		
1.3.	$\neg p$	
1.	$\neg q \rightarrow \neg p$	Direct Proof Rule
2.	$p \rightarrow q$	Contrapositive: 1

Proof by Contradiction: One way to prove $\neg$p

If we assume p and derive F (a contradiction), then we have proven $\neg$p.

1.1. p Assumption

…

1.3. F

1. $p \rightarrow$ F Direct Proof rule
2. $\neg p \vee$ F Law of Implication: 1
3. $\neg p$ Identity: 2

Proof Strategies: Proof by Contradiction

If we assume p and derive F (a contradiction), then we have proven ¬p.

We will argue by contradiction.

Suppose p.

…

This shows F, a contradiction.

1.1.	p	Assumption
…		
1.3.	F	
1.	$p \rightarrow$ F	Direct Proof rule
2.	$\neg p \vee$ F	Law of Implication: 1
3.	$\neg p$	Identity: 2

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y\ (x = 2y)$

Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse

Integers

Prove: "No integer is both even and odd."

Formally, prove $\neg \exists x\ (\text{Even}(x) \wedge \text{Odd}(x))$

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y\ (x = 2y)$

Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse

Integers

Prove: "No integer is both even and odd."

Formally, prove $\neg \exists x\,(\mathrm{Even}(x) \wedge \mathrm{Odd}(x))$

Proof: We work by contradiction. Suppose that x is an integer that is both even and odd.

Then, x=2a for some integer a and x=2b+1 for some integer b. This means 2a=2b+1 and hence a=b+½.

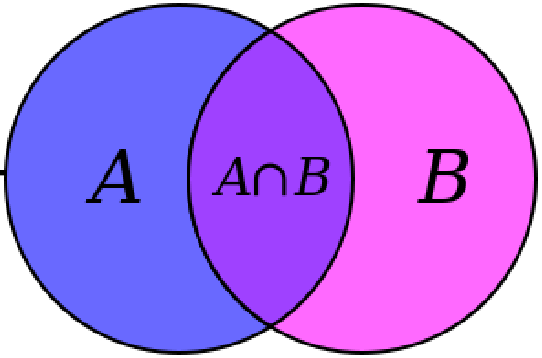
But two integers cannot differ by ½, so this is a contradiction. ■

Strategies

- Simple proof strategies already do a lot
  - counter examples
  - proof by contrapositive
  - proof by contradiction

- Later we will cover a specific strategy that applies to loops and recursion (mathematical induction)

Next Time: Set Theory



Sets are collections of objects called **elements.**

Write $a \in B$ to say that a is an element of set B, and $a \notin B$ to say that it is not.

Some simple examples

A = {1}

B = {1, 3, 2}

C = {□, 1}

D = {{17}, 17}

E = {1, 2, 7, cat, dog, ∅, α}