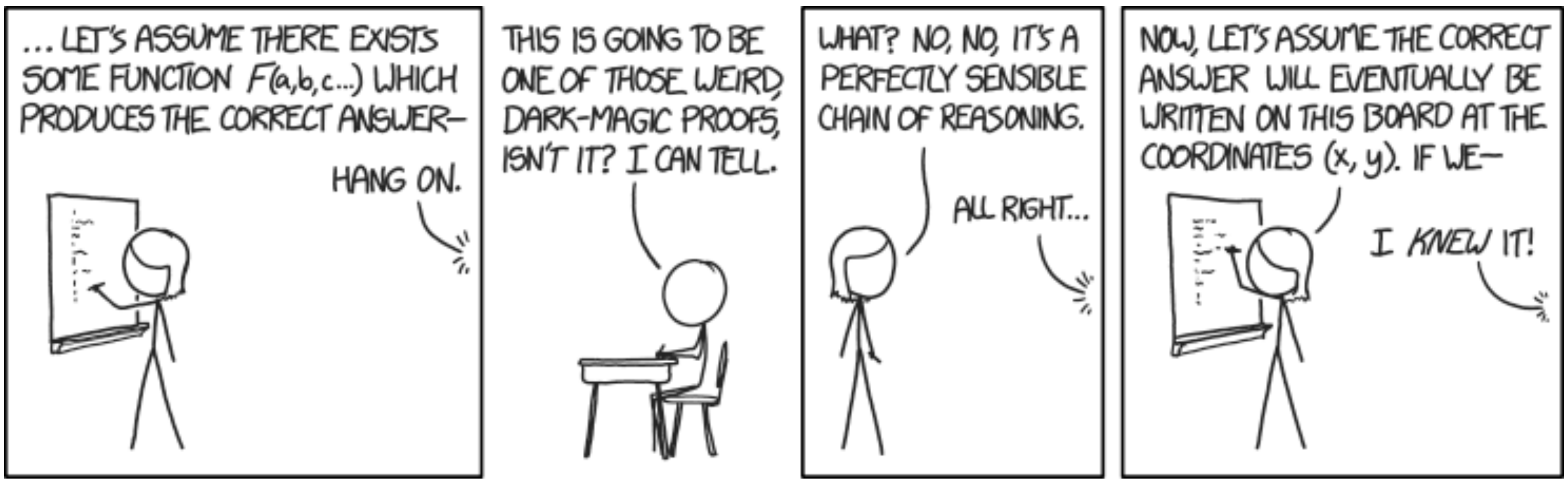
CSE 311: Foundations of Computing

Lecture 9: English Proofs & Proof Strategies



Last class: Inference Rules for Quantifiers

Intro ∃

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

Elim ∀

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

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 ∃

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

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

Dependencies

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

b depends on a since it appears inside the expression "$\exists y\, (y \geq \mathbf{a})$"

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 $\forall$: **1**
4. $\mathbf{b} \geq \mathbf{a}$ Elim $\exists$: **b** special depends on **a**
5. $\forall x\, (\mathbf{b} \geq x)$ Intro $\forall$: **2,4**
6. $\exists y \forall x\, (y \geq x)$ Intro $\exists$: **5**

Can't Intro $\forall$ **with "Let a be an arbitrary … P(a)"**
because P(a) = "$\mathbf{b} \geq \mathbf{a}$" uses object b, which depends on a!

Dependencies

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

b depends on a since it appears inside the expression "$\exists y\, (y \geq \mathbf{a})$"

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 $\forall$: 1
4.	$\mathbf{b} \geq \mathbf{a}$	Elim $\exists$: **b** special depends on **a**
5.	$\forall x\, (\mathbf{b} \geq x)$	Intro $\forall$: 2,4
6.	$\exists y \forall x\, (y \geq x)$	Intro $\exists$: 5

Have instead shown $\forall x\, (\mathbf{b}(x) \geq x)$

where $\mathbf{b}(x)$ is a number that is possibly different for each x

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	$\wedge$ Elim: 1
%d = load %c	Double Negation: 4
%e = add %arr, %i	$\vee$ Elim: 3, 5
store %e, %d	MP: 2, 6

Assembly Language for Programs	**Assembly Language for Proofs**

Proofs

Given

Given

$\wedge$ Elim: 1

Double Negation: 4

$\vee$ Elim: 3, 5

MP: 2, 6

what is the "Java" for proofs?

Assembly Language for Proofs

High-level Language for Proofs

Proofs

Given

Given

$\wedge$ Elim: 1

Double Negation: 4

$\vee$ 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 **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 $\exists$: **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 $\exists$ 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 $\forall$: 1,2

English Proof: Even and Odd

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

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** = 2**b** for some integer **b** (dep on **a**).	2.2	$\exists y\ (\mathbf{a} = 2y)$	Definition
	2.3	$\mathbf{a} = 2\mathbf{b}$	**b** special depends on **a**
Squaring both sides, we get $\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$.	2.4	$\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$	Algebra
So $\mathbf{a}^2$ is, by definition, even.	2.5	$\exists y\ (\mathbf{a}^2 = 2y)$	
	2.6	Even($\mathbf{a}^2$)	Definition
Since **a** was arbitrary, we have shown that the square of every even number is even.	2.	Even(**a**)$\rightarrow$Even($\mathbf{a}^2$)	
	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, $a = 2b$ for some integer b (depending on **a**). Squaring both sides, we get $a^2 = 4b^2 = 2(2b^2)$. So 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) $\equiv \exists y\ (x = 2y)$
Odd(x) $\equiv \exists y\ (x = 2y + 1)$

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) $\equiv \exists y\ (x = 2y)$

Odd(x) $\equiv \exists y\ (x = 2y + 1)$

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

Even(x) $\equiv \exists y\ (x=2y)$
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	$\text{Odd}(\mathbf{x}) \land \text{Odd}(\mathbf{y})$	Assumption
	2.2	$\text{Odd}(\mathbf{x})$	Elim $\land$: 2.1
	2.3	$\text{Odd}(\mathbf{y})$	Elim $\land$: 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 $\exists$: 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 $\exists$: 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 $\exists$: 2.4
	2.6	$\text{Odd}(\mathbf{b}^2)$	Def of Even
Since x and y were arbitrary, the sum of any odd integers is even.	2.	$\text{Odd}(\mathbf{b}) \to \text{Odd}(\mathbf{b}^2)$	
	3.	$\forall x\ (\text{Odd}(x) \to \text{Odd}(x^2))$	

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 $x = p/q$.

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

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."

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

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."

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

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

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.

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

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

Suppose that x and y are rational.

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

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

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

1.4 $\exists p\, \exists q\, ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$ **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."

...

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

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

...

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

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

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

...

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**

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

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."

...

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 $\wedge$: 1.5***
	1.12	$c \neq 0$	**Elim $\wedge$: 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) ≡ $\exists p\ \exists q\ ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

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

...

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

1.12 $\text{Integer}(b) \land (b \neq 0)$ — **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) $\equiv \exists p \, \exists q \, ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$

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

...

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

...

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

...

1.13 $b \neq 0$ — **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) $\equiv \exists p\ \exists q\ ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

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

...

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**

Furthermore, ac and bd are integers.

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

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

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. ■

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
  - reader checks that the writer is not skipping too much
  - examples so far
    - skipping Intro $\wedge$ and Elim $\wedge$
    - not stating existence claims (immediately apply Elim $\exists$ 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 reader 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: $\neg\forall \boldsymbol{x}\ \boldsymbol{P}(\boldsymbol{x}) \equiv \exists \boldsymbol{x} \neg \boldsymbol{P}(\boldsymbol{x})$
- All we need to do that is find an $\boldsymbol{x}$ where $\boldsymbol{P}(\boldsymbol{x})$ is **false**
- This example is called a ***counterexample*** to $\forall \boldsymbol{x}\ \boldsymbol{P}(\boldsymbol{x})$.

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 $\neg$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) $\equiv \exists y\ (x = 2y)$
Odd(x) $\equiv \exists y\ (x = 2y + 1)$

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

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.

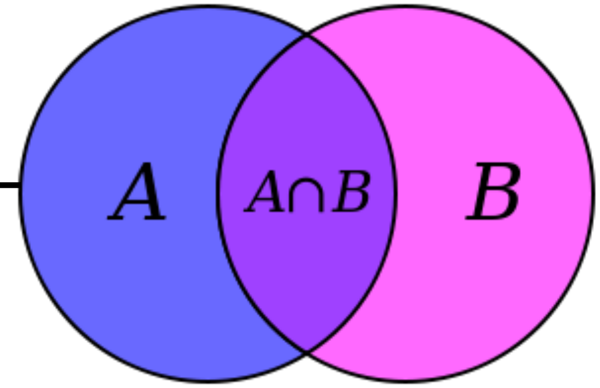
But two integers cannot differ by ½, so this is a contradiction. ■

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 ∈ B **to say that** a **is an element of set** B**,**
and a ∉ 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}