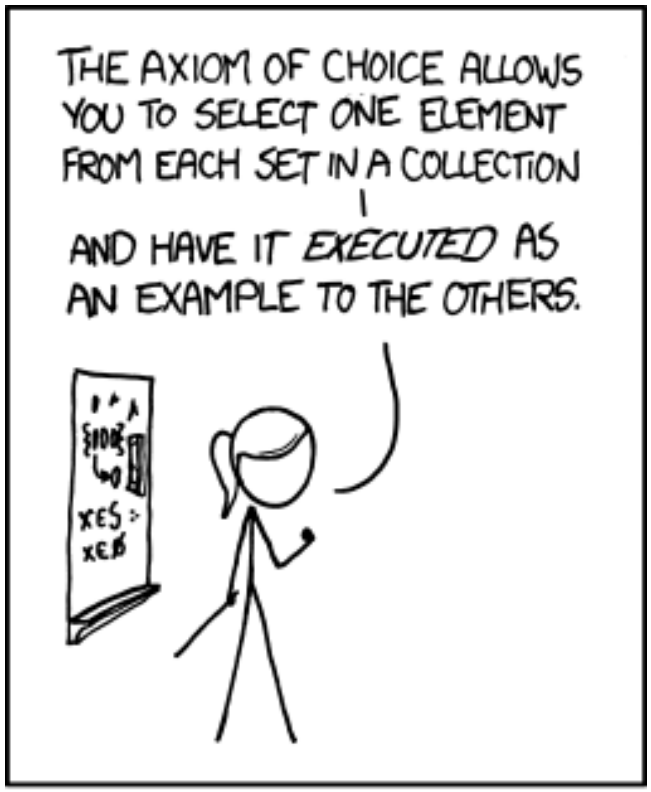
CSE 311: Foundations of Computing

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 ∀

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

Intro ∀

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

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

Elim ∃

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

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

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) / ∴ ∀x P(x)

* in the domain of P

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

** c has to be a NEW name.

Over integer domain: ∀x ∃y (y ≥ x) is True but ∃y∀x (y ≥ x) is False

BAD "PROOF"

1. ∀x ∃y (y ≥ x) — Given
2. Let a be an arbitrary integer
3. ∃y (y ≥ a) — Elim ∀: 1
4. b ≥ a — Elim ∃: b special depends on a
5. ∀x (b ≥ x) — Intro ∀: 2,4
6. ∃y∀x (y ≥ x) — Intro ∃ : 5

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) / ∴ ∀x P(x)

* in the domain of P

Elim ∃: ∃x P(x) / ∴ P(c) for some *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) / ∴ ∀x P(x)

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

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

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

Over integer domain: ∀x ∃y (y ≥ x) is True but ∃y∀x (y ≥ x) is False

BAD "PROOF"

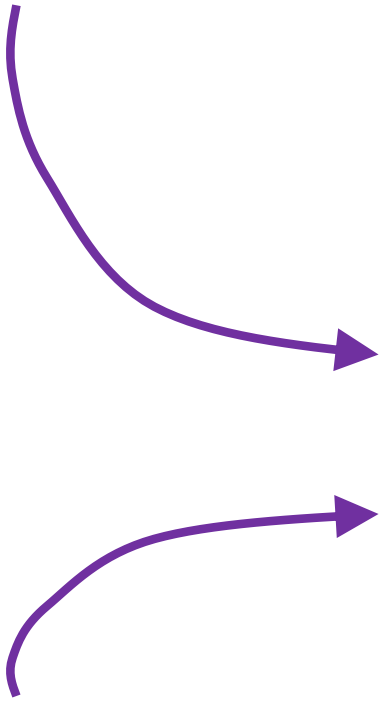
1. ∀x ∃y (y ≥ x) — Given
2. Let a be an arbitrary integer
3. ∃y (y ≥ a) — Elim ∀: 1
4. b ≥ a — Elim ∃: b special depends on a
5. ~~∀x (b ≥ x)~~ — ~~Intro ∀: 2,4~~
6. ∃y∀x (y ≥ x) — Intro ∃ : 5

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

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 "$\exists y\, (y \geq a)$"



BAD "PROOF"

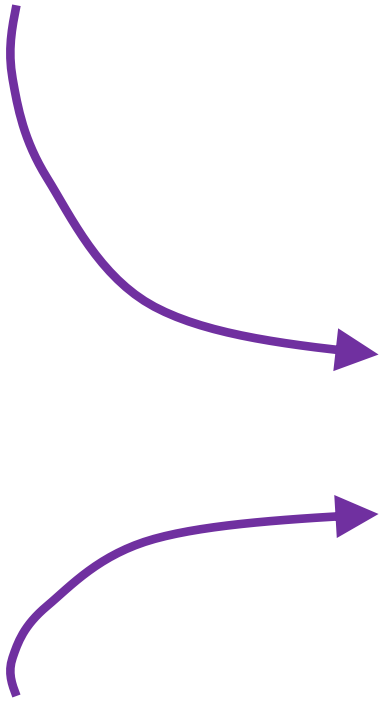
1.	$\forall x\, \exists y\, (y \geq x)$	Given
2.	Let a be an arbitrary integer	
3.	$\exists y\, (y \geq a)$	Elim $\forall$: 1
4.	$b \geq a$	Elim $\exists$: b special depends on a
5.	$\forall x\, (b \geq x)$	Intro $\forall$: 2,4
6.	$\exists y \forall x\, (y \geq x)$	Intro $\exists$: 5

Can't Intro $\forall$ with "Let a be an arbitrary … P(a)"
because P(a) = "$b \geq a$" 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 "$\exists y\, (y \geq a)$"



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

Have instead shown $\forall x\, (b(x) \geq x)$
where 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)
```

Assembly Language

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

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)`	Modus Ponens: 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 reader believes they could translate it into a formal proof**

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

Last class: Even and Odd

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

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

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

1. Let **a** be an arbitrary integer
   - 2.1 Even(**a**) — Assumption
   - 2.2 $\exists y\ (\mathbf{a} = 2y)$ — Definition of Even
   - 2.3 $\mathbf{a} = 2\mathbf{b}$ — 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 Even($\mathbf{a}^2$) — Definition of Even
2. $Even(\mathbf{a}) \rightarrow Even(\mathbf{a}^2)$ — Direct Proof
3. $\forall x\ (Even(x) \rightarrow Even(x^2))$ — Intro ∀: 1,2

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."

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 ∃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 ∃y (a^2 = 2y)

2.6 Even(a^2) Definition

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

2. Even(**a**)→Even(a^2)
3. ∀x (Even(x)→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** = 2**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. ■

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 **even** integer.

Then, by definition, $\mathbf{a} = 2\mathbf{b}$ for some integer b (dep 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. ■

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

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 "The sum of two odd numbers is even."

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

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."

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

Let x and y be arbitrary integers.

1. **Let x be an arbitrary integer**
2. **Let y be an arbitrary integer**

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

4. $\forall x\ \forall y\ ((\text{Odd}(\mathbf{x}) \wedge \text{Odd}(\mathbf{y})) \rightarrow \text{Even}(x+y))$ Intro $\forall$

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 $\forall x\ \forall y\ ((\text{Odd}(x) \wedge \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

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.

3.1 Odd(**x**) ∧ Odd(**y**) Assumption

so x+y is even.

3.9 Even(**x+y**)

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

3. (Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**) DPR
4. ∀x ∀y ((Odd(**x**) ∧ Odd(**y**)) → Even(x+y)) Intro ∀

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 $\forall x\ \forall y\ ((\text{Odd}(x) \wedge \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

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.

3.1	Odd(**x**) ∧ Odd(**y**)	Assumption
3.2	Odd(**x**)	Elim ∧: 2.1
3.3	Odd(**y**)	Elim ∧: 2.1

so x+y is even.

3.9 Even(**x+y**)

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

3.	(Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**)	DPR
4.	∀x ∀y ((Odd(**x**) ∧ Odd(**y**)) → Even(x+y))	Intro ∀

English Proof: Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃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.

3.1	Odd(**x**) ∧ Odd(**y**)	Assumption
3.2	Odd(**x**)	Elim ∧: 2.1
3.3	Odd(**y**)	Elim ∧: 2.1

Then, x = 2a+1 for some integer a (depending on x) and y = 2b+1 for some integer b (depending on y).

3.4	∃**z** (**x** = 2**z**+1)	Def of Odd: 2.2
3.5	**x** = 2**a**+1	Elim ∃: 2.4 (**a** dep **x**)
3.6	∃**z** (**y** = 2**z**+1)	Def of Odd: 2.3
3.7	**y** = 2**b**+1	Elim ∃: 2.5 (**b** dep **y**)

so x+y is, by definition, even.

3.9	∃z (**x**+**y** = 2z)	Intro ∃: 2.4
3.10	Even(**x**+**y**)	Def of Even

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

3.	(Odd(**x**) ∧ Odd(**y**)) → Even(**x**+**y**)	DPR
4.	∀x ∀y ((Odd(**x**) ∧ Odd(**y**)) → Even(**x**+**y**))	Intro ∀

English Proof: Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃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.

3.1	Odd(**x**) ∧ Odd(**y**)	Assumption
3.2	Odd(**x**)	Elim ∧: 2.1
3.3	Odd(**y**)	Elim ∧: 2.1

Then, x = 2a+1 for some integer a (depending on x) and y = 2b+1 for some integer b (depending on y).

3.4	∃**z** (**x** = 2**z**+1)	Def of Odd: 2.2
3.5	**x** = 2**a**+1	Elim ∃: 2.4 (**a** dep **x**)
3.6	∃**z** (**y** = 2**z**+1)	Def of Odd: 2.3
3.7	**y** = 2**b**+1	Elim ∃: 2.5 (**b** dep **y**)

Their sum is x+y = ... = 2(a+b+1)

3.8	**x+y** = 2(**a**+**b**+**1**)	Algebra

so x+y is, by definition, even.

3.9	∃z (**x+y** = 2z)	Intro ∃: 2.4
3.10	Even(**x+y**)	Def of Even

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

3.	(Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**)	DPR
4.	∀x ∀y ((Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**))	Intro ∀

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.

■

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 **odd** integers.

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. ■

$\forall x\ \forall y\ ((\text{Odd}(x) \wedge \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

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 $x = p/q$.**

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

Rationality

Domain of Discourse
Real Numbers

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

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

Formally, prove $\forall x\ \forall y\ ((\text{Rational}(x) \wedge \text{Rational}(y)) \rightarrow \text{Rational}(xy))$

Rationality

Domain of Discourse
Real Numbers

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

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

Proof: Let x and y be arbitrary rationals.

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

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

Proof: Let x and y be arbitrary rationals.

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

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

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

Proof: Let x and y be arbitrary rationals.

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 = (a/b)(c/d) = (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) := $\exists p\ \exists q\ (\text{Integer}(p) \wedge \text{Integer}(q) \wedge (x = p/q) \wedge (q \neq 0))$

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

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

Recall that unquantified variables (not constants) are implicitly for-all quantified.

Rationality

Domain of Discourse
Real Numbers

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

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

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

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**

1.2 $\text{Rational}(x)$ **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

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

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

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

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

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

1.8 $x = a/b$ **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) $\equiv \exists p\ \exists q\ ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$

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 ∧: 1.5***
	1.12 $d \neq 0$	**Elim ∧: 1.7**
Since b and d are non-zero, so is bd.	**1.13** $bd \neq 0$	**Prop of Integer Mult**

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

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

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

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

...

1.19 $\text{Integer}(a)$ — **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) $\equiv \exists p\ \exists q\ ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$

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

…

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

…

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

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

Intro ∧: 1.28, 1.30

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

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

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.

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

And finally...

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.

1.34 $\text{Rational}(xy)$ **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) := $\exists p\ \exists q\ (\text{Integer}(p) \wedge \text{Integer}(q) \wedge (x = p/q) \wedge (q \neq 0))$

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

Proof: Let x and y be arbitrary rationals.

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. ■

vs more than 35 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 ∧ 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 reader believes they could translate it into a formal proof
  - the reader is the "compiler" for English proofs