

# Logic and Interactive Theorem Proving

Jeremy Avigad

Department of Philosophy and  
Department of Mathematical Sciences  
Carnegie Mellon University

December 2015

# Mathematical language

---

Three notions of “mathematical language” :

- informal: ordinary mathematical writings, textbooks, journal articles
- formal: written in symbolic logic
- semiformal: stylized languages used by interactive proof assistants

## Informal proof

---

*Proof.* Suppose that  $E$  is a semistable elliptic curve over  $\mathbf{Q}$ . Assume first that the representation  $\bar{\rho}_{E,3}$  on  $E[3]$  is irreducible. Then if  $\rho_0 = \bar{\rho}_{E,3}$  restricted to  $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\sqrt{-3}))$  were not absolutely irreducible, the image of the restriction would be abelian of order prime to 3. As the semistable hypothesis implies that all the inertia groups outside 3 in the splitting field of  $\rho_0$  have order dividing 3 this means that the splitting field of  $\rho_0$  is unramified outside 3. However,  $\mathbf{Q}(\sqrt{-3})$  has no nontrivial abelian extensions unramified outside 3 and of order prime to 3. So  $\rho_0$  itself would factor through an abelian extension of  $\mathbf{Q}$  and this is a contradiction as  $\rho_0$  is assumed odd and irreducible. So  $\rho_0$  restricted to  $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\sqrt{-3}))$  is absolutely irreducible and  $\rho_{E,3}$  is then modular by Theorem 0.2 (proved at the end of Chapter 3). By Serre's isogeny theorem,  $E$  is also modular (in the sense of being a factor of the Jacobian of a modular curve).

So assume now that  $\bar{\rho}_{E,3}$  is reducible. Then we claim that the representation  $\bar{\rho}_{E,5}$  on the 5-division points is irreducible. This is because  $X_0(15)(\mathbf{Q})$  has only four rational points besides the cusps and these correspond to non-semistable curves which in any case are modular; cf. [BiKu, pp. 79–80]. If we knew that  $\bar{\rho}_{E,5}$  was modular we could now prove the theorem in the same way

## Informal proof

---

### Theorem

*Every natural number greater than equal to 2 can be written as a product of primes.*

### Proof.

We proceed by induction on  $n$ . Let  $n$  be any natural number greater than 2. If  $n$  is prime, we are done; we can consider  $n$  itself as a product with one term. Otherwise,  $n$  is composite, and we can write  $n = m \cdot k$  where  $m$  and  $k$  are smaller than  $n$ . By the inductive hypothesis, each of  $m$  can be written as a product of primes, say  $m = p_1 \cdot p_2 \cdot \dots \cdot p_u$  and  $k = q_1 \cdot q_2 \cdot \dots \cdot q_v$ . But then we have

$$n = m \cdot k = p_1 \cdot p_2 \cdot \dots \cdot p_u \cdot q_1 \cdot q_2 \cdot \dots \cdot q_v,$$

a product of primes, as required. □

## Informal proof

---

Theorem

$\sqrt{2}$  is irrational.

Proof.

Suppose  $\sqrt{2} = a/b$  for some pair of integers  $a$  and  $b$ . By removing any common factors, we can assume  $a/b$  is in lowest terms, so that  $a$  and  $b$  have no factor in common. Then  $a = \sqrt{2}b$ , and squaring both sides, we have  $a^2 = 2b^2$ .

The last equation implies that  $a^2$  is even, and since the square of an odd number is odd,  $a$  itself must be even as well. We therefore have  $a = 2c$  for some integer  $c$ . Substituting this into the equation  $a^2 = 2b^2$ , we have  $4c^2 = 2b^2$ , and hence  $2c^2 = b^2$ . This means that  $b^2$  is even, and so  $b$  is even as well.

The fact that  $a$  and  $b$  are both even contradicts the fact that  $a$  and  $b$  have no common factor. So the original assumption that  $\sqrt{2} = a/b$  is false. □

## Formal proof

---

Natural deduction in symbolic logic gives an idealized model of reasoning:

$$\frac{\frac{\frac{\neg \text{even}(b)}{\quad}}{\quad} \quad \frac{\frac{\forall x (\neg \text{even}(x) \rightarrow \neg \text{even}(x^2))}{\quad} \quad \frac{\neg \text{even}(b) \rightarrow \neg \text{even}(b^2))}{\quad}}{\neg \text{even}(b^2)} \quad \text{even}(b^2)}{\frac{\perp}{\text{even}(b)}}$$

## Semiformal proof

---

```
theorem sqrt_two_irrational {a b : ℕ} (co : coprime a b) :
  a^2 ≠ 2 * b^2 :=
  assume H : a^2 = 2 * b^2,
  have even (a^2), from even_of_exists (exists.intro _ H),
  have even a, from even_of_even_pow this,
  obtain (c : nat) (aeq : a = 2 * c), from exists_of_even this,
  have 2 * (2 * c^2) = 2 * b^2,
    by rewrite [-H, aeq, *pow_two, algebra.mul.assoc, algebra.mul.
      left_comm c],
  have 2 * c^2 = b^2, from eq_of_mul_eq_mul_left dec_trivial this,
  have even (b^2),
    from even_of_exists (exists.intro _ (eq.symm this)),
  have even b, from even_of_even_pow this,
  assert 2 | gcd a b,
    from dvd_gcd (dvd_of_even 'even a') (dvd_of_even 'even b'),
  have 2 | 1,
    by rewrite [gcd_eq_one_of_coprime co at this]; exact this,
  show false, from absurd '2 | 1' dec_trivial
```

# Mathematical language

---

What they are good for:

- Informal language: ordinary communication, reading, and understanding
- Formal language: reasoning *about* mathematical reasoning, studying its properties
- Semiformal language: implementation, interaction with computers

Semiformal languages are between the other two:

- more precise than informal language
- more expressive than symbolic logic



# Mathematical language

---

Two different aspects of mathematical language:

- assertion language: making mathematical statements
- proof language: writing mathematical proofs

An assertion:

- Every prime number greater than 2 is odd.
- $\forall n \text{ prime}(n) \wedge n > 2 \rightarrow \text{odd}(n)$ .
- $\forall n, \text{prime } n \rightarrow n > 2 \rightarrow \text{odd } n$

# First-order logic

---

We start with a *language*, that is, a specification of constant symbols, function symbols, and relation symbols.

For example, we will consider the following “language of arithmetic”:

- Constant symbols:  $0, 1, 2, \dots$
- Function symbols:  $+, \times$ , exponentiation
- Predicates and relations:  $=, <, \leq, |$ , *even*, *odd*, *prime*,  $\dots$

Intuitively, we have designed this language to talk about  $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ .

Formally, we are just dealing with symbols.

## First-order logic

---

Once we have specified the language, we get a set of *terms*:

- Start with variables and constant symbols.
- Build more complex terms with function symbols.

Examples:  $x$ ,  $0$ ,  $(x + y) \times 0$ ,  $x \times 2 + y \times 0$ ,  $\dots$

Intuition: terms name elements of the intended universe, modulo an assignment of values to the free variables.

# First-order logic

---

We also get *formulas*:

- Start with basic predicates and relations on terms.
- Build more complex formulas:
  - $P \wedge Q$ : “ $P$  and  $Q$ ”
  - $P \vee Q$ : “ $P$  or  $Q$ ”
  - $P \rightarrow Q$ : “if  $P$  then  $Q$ ”
  - $\neg P$ : “not  $P$ ”
  - $\forall x P$ : “for every  $x$ ,  $P$ ”
  - $\exists x P$ : “for some  $x$ ,  $P$ ”

Examples:  $s = t \wedge 0 < s$ ,  $prime(x)$ ,  $\forall x \exists y (x < y \wedge y < x + 2)$

Intuition: formulas say things about the intended universe, modulo an assignment of values to the free variables.

## First-order logic

---

Every natural number is even or odd, but not both.

## First-order logic

---

Every natural number is even or odd, but not both.

$$\forall x ((\text{even}(x) \vee \text{odd}(x)) \wedge \neg(\text{even}(x) \wedge \text{odd}(x)))$$

## First-order logic

---

Every natural number is even or odd, but not both.

$$\forall x ((\text{even}(x) \vee \text{odd}(x)) \wedge \neg(\text{even}(x) \wedge \text{odd}(x)))$$

If some natural number,  $x$ , is even, then so is  $x^2$ .

## First-order logic

---

Every natural number is even or odd, but not both.

$$\forall x ((\text{even}(x) \vee \text{odd}(x)) \wedge \neg(\text{even}(x) \wedge \text{odd}(x)))$$

If some natural number,  $x$ , is even, then so is  $x^2$ .

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



## First-order logic

---

Every natural number is even or odd, but not both.

$$\forall x ((\text{even}(x) \vee \text{odd}(x)) \wedge \neg(\text{even}(x) \wedge \text{odd}(x)))$$

If some natural number,  $x$ , is even, then so is  $x^2$ .

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

For any three natural numbers  $x$ ,  $y$ , and  $z$ , if  $x$  divides  $y$  and  $y$  divides  $z$ , then  $x$  divides  $z$ .

## First-order logic

---

Every natural number is even or odd, but not both.

$$\forall x ((\text{even}(x) \vee \text{odd}(x)) \wedge \neg(\text{even}(x) \wedge \text{odd}(x)))$$

If some natural number,  $x$ , is even, then so is  $x^2$ .

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

For any three natural numbers  $x$ ,  $y$ , and  $z$ , if  $x$  divides  $y$  and  $y$  divides  $z$ , then  $x$  divides  $z$ .

$$\forall x, y, z (x \mid y \wedge y \mid z \rightarrow x \mid z)$$

## First-order logic

---

Every natural number is even or odd, but not both.

$$\forall x ((\text{even}(x) \vee \text{odd}(x)) \wedge \neg(\text{even}(x) \wedge \text{odd}(x)))$$

If some natural number,  $x$ , is even, then so is  $x^2$ .

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

For any three natural numbers  $x$ ,  $y$ , and  $z$ , if  $x$  divides  $y$  and  $y$  divides  $z$ , then  $x$  divides  $z$ .

$$\forall x, y, z (x \mid y \wedge y \mid z \rightarrow x \mid z)$$

For every  $x > 1$ , there is a prime number between  $x$  and  $2x$ .

## First-order logic

---

Every natural number is even or odd, but not both.

$$\forall x ((\text{even}(x) \vee \text{odd}(x)) \wedge \neg(\text{even}(x) \wedge \text{odd}(x)))$$

If some natural number,  $x$ , is even, then so is  $x^2$ .

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

For any three natural numbers  $x$ ,  $y$ , and  $z$ , if  $x$  divides  $y$  and  $y$  divides  $z$ , then  $x$  divides  $z$ .

$$\forall x, y, z (x \mid y \wedge y \mid z \rightarrow x \mid z)$$

For every  $x > 1$ , there is a prime number between  $x$  and  $2x$ .

$$\forall x (x > 1 \rightarrow \exists y (\text{prime}(y) \wedge x < y \wedge y < 2 \times x))$$

## First-order logic

---

Every natural number is even or odd, but not both.

$$\forall x, ((\text{even } x \vee \text{odd } x) \wedge \neg(\text{even } x \wedge \text{odd } x))$$

If some natural number,  $x$ , is even, then so is  $x^2$ .

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

For any three natural numbers  $x$ ,  $y$ , and  $z$ , if  $x$  divides  $y$  and  $y$  divides  $z$ , then  $x$  divides  $z$ .

$$\forall x \ y \ z, x \mid y \rightarrow y \mid z \rightarrow x \mid z$$

For every  $x > 1$ , there is a prime number between  $x$  and  $2x$ .

$$\forall x, (x > 1 \rightarrow \exists y, \text{prime } y \wedge x < y \wedge y < 2 * x)$$

## Natural deduction

---

A formal system called *natural deduction*, designed by Gerhard Gentzen, provides a nice formal model of mathematical proof.

The basic notion: a proof from *hypotheses*.

A complex proof is built up from simpler proofs using logical rules.

Over the course of a proof, hypotheses can change.

For example, we can temporarily assume  $A$  in order to prove  $A \rightarrow B$ .

# Natural deduction

---

$$\frac{\begin{array}{c} \overline{A}^a \\ \vdots \\ B \end{array}}{A \rightarrow B}^a \rightarrow\text{I} \qquad \frac{A \rightarrow B \quad A}{B} \rightarrow\text{E}$$

$$\frac{A \quad B}{A \wedge B} \wedge\text{I} \qquad \frac{A \wedge B}{A} \wedge\text{E}_1 \qquad \frac{A \wedge B}{B} \wedge\text{E}_r$$

$$\frac{\begin{array}{c} \overline{A}^a \\ \vdots \\ \perp \end{array}}{\neg A}^a \neg\text{I} \qquad \frac{\neg A \quad A}{\perp} \neg\text{E}$$

# Natural deduction

---

$$\frac{A}{A \vee B} \vee I_1$$

$$\frac{B}{A \vee B} \vee I_2$$

$$\frac{\begin{array}{cc} \overline{A}^a & \overline{B}^b \\ \vdots & \vdots \\ A \vee B & C \end{array}}{C} \vee E$$

$$\frac{\perp}{A} \perp E$$

$$\frac{\begin{array}{c} \overline{\neg A}^a \\ \vdots \\ \perp \end{array}}{A} \text{RAA}$$



# Natural deduction

---

$$\frac{A(x)}{\forall y A(y)} \forall I$$

$$\frac{\forall x A(x)}{A(t)} \forall E$$

$$\frac{A(t)}{\exists x A(x)} \exists I$$

$$\frac{\exists x A(x) \quad \begin{array}{c} \overline{A(y)}^a \\ \vdots \\ B \end{array}}{B} a \exists E$$

## Examples

---

We'll do some of these in natural deduction, and in *Lean*:

- show  $A \wedge B \rightarrow B \wedge A$
- show  $A \rightarrow C$ , assuming  $A \rightarrow B$  and  $B \rightarrow C$
- show  $B$ , assuming  $A \vee B$  and  $\neg A$
- show  $C$ , assuming  $A \vee B$ ,  $A \rightarrow C$ , and  $B \rightarrow C$
- show  $\forall x (A(x) \wedge B(x)) \rightarrow \forall x A(x)$
- show  $\neg \exists x A(x) \rightarrow \forall x \neg A(x)$

## Beyond first-order logic

---

What if we want a system to do *all of mathematics*, not just reason about the natural numbers?

Two options:

- Set theory: write down a powerful set of axioms describing sets. Show that ordinary mathematical objects (numbers, functions, relations, points, lines, triangles, groups, hyperbolic manifolds, ...) can be defined as various kinds of sets.
- Type theory: extend first-order logic with constructions for functions, propositions, and inductive definitions, and construct mathematical objects from those.

The two approaches are essentially inter-translatable.

Interactive theorem provers usually use a variant of type theory.