FIRST-ORDER PREDICATE LOGIC

Special Topics

Wolfgang Schreiner and Wolfgang Windsteiger
Wolfgang.(Schreiner|Windsteiger)@risc.jku.at
Research Institute for Symbolic Computation (RISC)
Johannes Kepler University (JKU), Linz, Austria
http://www.risc.jku.at

Special Topics

We will conclude by discussing the following special topics:

- the method of induction for reasoning about natural numbers,
- the expressiveness and limits of first-order predicate logic.

Mathematical Induction

A method to prove statements over the natural numbers ($\mathbb{N}_{\geq m} = \{m, m+1, m+2, \ldots\}$).

- Goal: prove

$$\forall n \in \mathbb{N}_{\geq m} : F$$

- Rule:

$$\frac{K \ldots \ \vdash \ F[m/n] \qquad K \ldots, \overline{n} \in \mathbb{N}_{\geq m}, F[\overline{n}/n] \ \vdash \ F[(\overline{n}+1)/n]}{K \ldots \ \vdash \ \forall n \in \mathbb{N}_{\geq m} : F}$$

  $F[t/n]$: F where every free occurrence of n is replaced by t.

- Proof Steps:
  - Induction base: prove that F holds for m.
  - Induction hypothesis: assume that F holds for new constant $\overline{n} \geq m$.
  - Induction step: prove that then F also holds for $\overline{n}+1$.

Every $n \geq m$ is reachable by a finite number of increments starting from m.

Example

We prove the "sum of squares" formula $\forall n \in \mathbb{N}\colon \sum_{i=1}^{n} i^2 = \frac{n \cdot (n+1) \cdot (2n+1)}{6}$

- Induction Base: in this case $m = 0$.

$$\sum_{i=1}^{0} i^2 = 0 = \frac{0 \cdot (0+1)(2 \cdot 0+1)}{6}$$

- Induction Hypothesis: assume

$$\sum_{i=1}^{\overline{n}} i^2 = \frac{\overline{n} \cdot (\overline{n}+1) \cdot (2\overline{n}+1)}{6} \qquad (*)$$

- Induction Step: prove

$$\sum_{i=1}^{\overline{n}+1} i^2 = (\overline{n}+1)^2 + \sum_{i=1}^{\overline{n}} i^2 \stackrel{(*)}{=} (\overline{n}+1)^2 + \frac{\overline{n} \cdot (\overline{n}+1) \cdot (2\overline{n}+1)}{6} = \frac{(\overline{n}+1) \cdot (6 \cdot (\overline{n}+1) + \overline{n} \cdot (2\overline{n}+1))}{6} =$$

$$= \frac{(\overline{n}+1) \cdot (2\overline{n}^2 + 7\overline{n} + 6)}{6} = \frac{(\overline{n}+1) \cdot (\overline{n}+2) \cdot (2\overline{n}+3)}{6} = \frac{(\overline{n}+1) \cdot ((\overline{n}+1)+1) \cdot (2(\overline{n}+1)+1)}{6} \qquad \square$$

Example

We prove

$$\forall n \in \mathbb{N}_{n \geq 4} \colon n^2 \leq 2^n$$

- Induction base: in this case $m = 4$, i.e., we show
$$4^2 = 16 = 2^4.$$
- Induction hypothesis: we assume for $n \geq 4$
$$n^2 \leq 2^n. \qquad (*)$$
- Induction step: we show
$$(n+1)^2 = n^2 + 2n + 1 \overset{1 \leq n}{\leq} n^2 + 2n + n = n^2 + 3n \overset{0 \leq n}{\leq} n^2 + 4n$$
$$\overset{4 \leq n}{\leq} n^2 + n \cdot n = n^2 + n^2 = 2n^2 \overset{(*)}{\leq} 2 \cdot 2^n = 2^{n+1}. \quad \square$$

Choice of Induction Variable

We define addition on $\mathbb{N}$ by primitive recursion:

$$x + 0 := x \tag{1}$$

$$x + (y + 1) := (x + y) + 1 \tag{2}$$

Our goal is to prove the associativity law

$$\forall x \in \mathbb{N}, y \in \mathbb{N}, z \in \mathbb{N} \colon x + (y + z) = (x + y) + z$$

For this purpose, we fix arbitrary $x_0, y_0 \in \mathbb{N}$ and then prove

$$\forall z \in \mathbb{N} \colon x_0 + (y_0 + z) = (x_0 + y_0) + z$$

by induction on z.

Sometimes the appropriate choice of the induction variable is critical.

Choice of Induction Variable

We prove by induction on z: $\forall z \in \mathbb{N}\colon x_0 + (y_0 + z) = (x_0 + y_0) + z.$

- Induction base: we prove

$$x_0 + (y_0 + 0) \overset{(1)}{=} x_0 + y_0 \overset{(1)}{=} (x_0 + y_0) + 0.$$

- Induction hypothesis: we assume for $z_0 \in \mathbb{N}$

$$x_0 + (y_0 + z_0) = (x_0 + y_0) + z_0. \qquad (*)$$

- Induction step: we have to show $x_0 + (y_0 + (z_0 + 1)) = (x_0 + y_0) + (z_0 + 1).$

$$x_0 + (y_0 + (z_0 + 1)) \overset{(2)}{=} x_0 + ((y_0 + z_0) + 1) \overset{(2)}{=} (x_0 + (y_0 + z_0)) + 1 =$$
$$\overset{(*)}{=} ((x_0 + y_0) + z_0) + 1 \overset{(2)}{=} (x_0 + y_0) + (z_0 + 1). \quad \square$$

Expressiveness of First-Order Logic (I)

- Variables denote elements of the domain, thus no quantification is possible over functions and predicates of the domain.
  This would require second-order predicate logic.

- Nevertheless we express in first-order logic statements such as

  $$\forall A, B, f\colon \mathsf{isFun}(f, A, B) \land \mathsf{bijective}(f) \to \exists g\colon \mathsf{isFun}(g, B, A) \land \forall x \in B\colon f(g(x)) = x$$

  where $\mathsf{isFun}(f, A, B)$ and $\mathsf{isFun}(g, B, A)$ express that
  - f and g are functions from A to B and from B to A, respectively.

Expressiveness of First-Order Logic (II)

- This is possible because formulas are usually interpreted over the domain of sets, i.e., all variables denote sets, e.g., $\mathsf{isFun}(f,A,B)$ means $f \subseteq A \times B$ s.t.

$$\forall a \in A\colon \exists b \in B\colon (a,b) \in f$$
$$\forall a,b,b'\colon (a,b) \in f \wedge (a,b') \in f \rightarrow b = b'.$$

- Terms like $f(g(x))$ involve a hidden binary function "apply" ("function application")

$$f(g(x)) \rightsquigarrow \mathsf{apply}(f,\mathsf{apply}(g,x))$$

with

$$\mathsf{apply}(f,x) := \textbf{the}\ y\colon (x,y) \in f.$$

- Set theory pushes functions down to the level of objects.
- First-order predicate logic over the domain of sets is the "working horse" of mathematics; virtually all of mathematics is formulated in this framework.

Limitations of FO Logic: Soundness and Completeness

Completeness Theorem (Kurt Gödel, 1929): First-order predicate logic has a proof calculus for which the following holds:

- Soundness: if a conclusion F can be derived from a set of assumptions Γ by the rules of the calculus, then F is a logical consequence of Γ, i.e.,

  $$\text{if } \Gamma \vdash F \text{ then } \Gamma \models F.$$

- Completeness: if F is a logical consequence of Γ, then F can be derived from Γ by the rules of the calculus, i.e.,

  $$\text{if } \Gamma \models F \text{ then } \Gamma \vdash F.$$

No logic that is stronger (more expressive) than first-order predicate logic has a proof calculus that also enjoys both soundness and completeness.

Undecidability of First-Order Logic

The existence of a complete proof calculus does not mean that the truth of every formula is algorithmically decidable.

- Undecidability (Church/Turing, 1936/1937): there does not exist any algorithm that for given formula set Γ and formula F always terminates and says whether $\Gamma \models F$ holds or not.
- Semidecidability: but there exists an algorithm, that for given Γ and F, if $\Gamma \models F$, detects this fact in a finite amount of time.
  This algorithm searches for a proof of $\Gamma \vdash F$ in a complete proof calculus; if such a proof exists, it will eventually detect it; however, if no such proof exists, the search runs forever.

Automatic proof search is not able to detect that a formula is not true.

Limits of First-Order Logic

Not every structure can be completely described by a finite set of formulas.

- Incompleteness Theorem (Kurt Gödel, 1931): it is in no sound logic possible to prove all true arithmetic statements (i.e., all statements about natural numbers with addition and multiplication).
  - To adequately characterize $\mathbb{N}$, the (infinite) axiom scheme of mathematical induction has to be added.
- Corollary: in every sound formal system that is sufficiently rich there are statements that can neither be proved nor disproved.

In practice, complete reasoners for first-order logic are often supported by (complete or incomplete) reasoners for special theories.