Computer Supported Modeling and Reasoning

David Basin, Achim D. Brucker, Jan-Georg Smaus, and Burkhart Wolff

April 2005

http://www.infsec.ethz.ch/education/permanent/csmr/

First-Order Logic: Theories

David Basin, Burkhart Wolff, and Jan-Georg Smaus

Overview

Last lecture: first-order logic.

This lecture:

- first-order logic with equality and first-order theories;
- set-theoretic reasoning.

We extend language and deductive system to formalize and reason about the (mathematical) world.

FOL with Equality

Equality is a logical symbol rather than a mathematical one.

Speak of first-order logic with equality rather than adding equality as “just another predicate”.

Syntax and Semantics

Syntax: $=$ is a binary infix predicate.

$t_1 = t_2 \in \mathit{Form}$ if $t_1, t_2 \in \mathit{Term}$.

Semantics : recall a structure is a pair $\mathcal{A} = \langle U_{\mathcal{A}}, I_{\mathcal{A}} \rangle$ and $I_{\mathcal{A}}(t)$ is the interpretation of t.

$$I_{\mathcal{A}}(s = t) = \begin{cases} 1 & \text{if } I_{\mathcal{A}}(s) = I_{\mathcal{A}}(t) \\ 0 & \text{otherwise} \end{cases}$$

Note the three completely different uses of "$=$" here!

Rules

- Equality is an equivalence relation

$$\frac{}{x = x}\ \textit{refl} \qquad \frac{x = y}{y = x}\ \textit{sym} \qquad \frac{x = y \quad y = z}{x = z}\ \textit{trans}$$

- Equality is also a congruence on terms and all relations

$$\frac{x_1 = y_1 \quad \cdots \quad x_n = y_n}{t(x_1, \ldots, x_n) = t(y_1, \ldots, y_n)}\ \textit{cong}_1$$

$$\frac{x_1 = y_1 \quad \cdots \quad x_n = y_n \quad A(x_1, \ldots, x_n)}{A(y_1, \ldots, y_n)}\ \textit{cong}_2$$

Congruence: Alternatives

One can specialize congruence rules to replace only some term occurrences.

$$\frac{x_1 = y_1 \quad \cdots \quad x_n = y_n}{t[z_1 \leftarrow x_1, \ldots, z_n \leftarrow x_n] = t[z_1 \leftarrow y_1, \ldots, z_n \leftarrow y_n]}\ \mathit{cong}_1$$

$$\frac{x_1 = y_1 \quad \cdots \quad x_n = y_n \quad A[z_1 \leftarrow y_1, \ldots, z_n \leftarrow y_n]}{A[z_1 \leftarrow x_1, \ldots, z_n \leftarrow x_n]}\ \mathit{cong}_2$$

One time the z's are replaced with x's and one time with y's.

Examples

How many ways are there to choose some occurrences of x in $x^2 + y^2 > 12 \cdot x$? 4, namely:

$$A = x^2 + y^2 > 12 \cdot x, \quad A = z^2 + y^2 > 12 \cdot x,$$
$$A = x^2 + y^2 > 12 \cdot z, \quad A = z^2 + y^2 > 12 \cdot z.$$

We show two ways:

$$\frac{x = 3 \quad x^2 + y^2 > 12 \cdot x}{3^2 + y^2 > 12 \cdot x} \text{ with } A = z^2 + y^2 > 12 \cdot x$$

$$\frac{x = 3 \quad x^2 + y^2 > 12 \cdot x}{x^2 + y^2 > 12 \cdot 3} \text{ with } A = x^2 + y^2 > 12 \cdot z$$

Isabelle Rule

The Isabelle FOL rule is simply (using a tree syntax)

$$\frac{x = y \quad P(x)}{P(y)}\ \textit{subst}$$

or literally

$$[\![a = b; P(a)]\!] \Longrightarrow P(b)$$

Proving $\exists x.\, t = x$

$$\dfrac{\dfrac{}{t = t}\,\textit{refl}}{\exists x.\, t = x}\,\exists\text{-}I$$

In the rule $\dfrac{A(t)}{\exists x.\, A(x)}\,\exists\text{-}I$, "$A(x)$" is metanotation. In the example, $A(x) = (t = x)$.

Notational confusion avoided by a precise metalanguage.

More Detailed Explanations

Logical vs. Non-logical Symbols

In logic languages, it is common to distinguish between logical and non-logical symbols. We explain this for first-order logic.

Recall that there isn't just the language of first-order logic, but rather defining a particular signature gives us a first-order language. The logical symbols are those that are part of any first-order language and whose meaning is "hard-wired" into the formalism of first-order logic, like $\wedge$ or $\forall$. The non-logical symbols are those given by a particular signature, and whose meaning must be defined "by the user" by giving a structure.

What status should the equality symbol $=$ have? We will assume that $=$ is a symbol whose meaning is hard-wired into the formalism. One then speaks of first-order logic with equality.

Three Different Uses of Equality

$$I_{\mathcal{A}}(s=t) = \begin{cases} 1 & \text{if } I_{\mathcal{A}}(s)=I_{\mathcal{A}}(t) \\ 0 & \text{otherwise} \end{cases}$$

The first $=$ is a predicate symbol.

The second $=$ is a definitional occurrence: The expression on the left-hand side is defined to be equal to the value of the right-hand side.

The third $=$ is semantic equality, i.e., the identity relation on the domain.

Why Rules?

Since $=$ is a logical symbol in the formalism of first-order logic with equality, there should be derivation rules for $=$ to derive which formulas $a = b$ are true.

What is an Equivalence?

In general mathematical terminology, a relation $\cong$ is an equivalence relation if the following three properties hold:

Reflexivity: $a \cong a$ for all a;

Symmetry: $a \cong b$ implies $b \cong a$;

Transitivity: $a \cong b$ and $b \cong c$ implies $a \cong c$.

Example: being equal modulo 6.
"a is equal b modulo 6" is often written $a \equiv b \bmod 6$.

What is a Congruence?

In general mathematical terminology, a relation $\cong$ is a congruence w.r.t. (or: on) f, where f has arity n, if $a_1 \cong b_1, \ldots, a_n \cong b_n$ implies $f(a_1, \ldots, a_n) \cong f(b_1, \ldots, b_n)$.

Example: being equal modulo 6 is congruent w.r.t. multiplication.

$14 \equiv 8 \bmod 6$ and $15 \equiv 9 \bmod 6$, hence $14 \cdot 15 \equiv 8 \cdot 9 \bmod 6$.

This can be defined in an analogous way for a property (relation) P.

Example: being equal modulo 6 is congruent w.r.t. divisibility by 3.

$15 \equiv 9 \bmod 6$ and 15 is divisible by 3, hence 9 is divisible by 3.

$14 \equiv 8 \bmod 6$ and 14 is not divisible by 3, hence 8 is not divisible by 3.

Soundness of Equivalence Rules

On the semantic level, two things are equal if they are identical.

Semantic equality is an equivalence relation.

So one can prove that $I_{\mathcal{A}}(s = s) = 1$ for all all terms s, because $I_{\mathcal{A}}(s) = I_{\mathcal{A}}(s)$ for all terms, and likewise for symmetry and transitivity.

Soundness of Congruence Rules

If $t(x)$ is a term containing x and $t(y)$ is the term obtained from $t(x)$ by replacing all occurrences of x with y, and moreover $I_{\mathcal{A}}(x = y) = 1$, then $I_{\mathcal{A}}(x) = I_{\mathcal{A}}(y)$. One can show by induction on the structure of t that $I_{\mathcal{A}}(t(x)) = I_{\mathcal{A}}(t(y))$.

So by “truth-functional” we mean that the value $I_{\mathcal{A}}(t(x))$ depends on $I_{\mathcal{A}}(x)$, not on x itself.

This can be generalized to n variables as in the rule.

An analogous proof can be done for rule *cong*$_2$.

Occurrences vs. Substitution

The notation $t[z_1 \leftarrow x_1, \dots, z_n \leftarrow x_n]$ stands for the term obtained from t by simultaneously replacing each z_i ($i \in \{1, \dots, n\}$) with x_i.

$[z_1 \leftarrow x_1, \dots, z_n \leftarrow x_n]$ is called a substitution.

Substitutions are a way to make the notion of variable occurence precise: assume we have a term t containing the (free) variable x.

Now, we can represent the n occurences of x in t by terms t_1 to t_n, for which $t = t_i[z \longleftarrow x]$ holds, where z is not a free variable in t and where z appears only once in the term. Then, the t_i represents an occurrence of x in t which is marked by z.

See also example.

Example: $x^2 + y^2 > 12 \cdot x$

The atom $x^2 + y^2 > 12 \cdot x$ contains two occurrences of x. There are four ways to choose some occurrences of x in $x^2 + y^2 > 12 \cdot x$.

Each of those ways corresponds to an atom obtained from $x^2 + y^2 > 12 \cdot x$ by replacing some occurrences of x with z. That is, there are four different A's such that $A[x \longleftarrow z] = x^2 + y^2 > 12 \cdot x$.

Now the atom above the line in the examples is obtained by substituting x for z, and the atom below the line is obtained by substituting y for z.

The Substitutivity Rule

The FOL rule for Substitutivity ("Leipnitz Rule") is presented as:

$$\frac{x = y \quad P(x)}{P(y)}\ \textit{subst}$$

We can think of $P(x)$ and $P(y)$ as $P[z \longleftarrow x]$ for some arbitrary z. Think of P as a formula where some positions are marked in such a way that once we apply P to t (we write $P(t)$), t will be substituted into all those positions.

In fact, the particular choice of z does not play a role; it is an "anonymous" variable from the point of view of substitutivity. This motivates the λ-calculus which allows for writing $\lambda z.P$ for this situation.

Why Are All Functions in a Structure Total?

If we allowed partial functions in a structure, then terms t can be undefined, and elementary operations like substitution require all sorts of side-conditions (we must not replace a variable with an undefined term, etc.).

First-Order Theories

David Basin, Burkhart Wolff, and Jan-Georg Smaus

Example 1: Partial Orders

- The language of the theory of partial orders: $\leq$
- Axioms

$$\forall x, y, z.\, x \leq y \wedge y \leq z \rightarrow x \leq z$$
$$\forall x, y.\, x \leq y \wedge y \leq x \leftrightarrow x = y$$

- Alternative to axioms is to convert to rules

$$\frac{x \leq y \quad y \leq z}{x \leq z}\ \textit{trans} \qquad \frac{x \leq y \quad y \leq x}{x = y}\ \textit{antisym} \qquad \frac{x = y}{x \leq y}\ \leq\textit{-refl}$$

Such a conversion is possible since implication is the main connective.

A Second Transitivity Rule

One may also consider adding the rule

$$\frac{x = y}{y \leq x} \ \leq\text{-}\mathit{refl2}$$

to the system. This rule can be derived as follows:

$$\dfrac{\dfrac{x = y}{y = x}\ \mathit{sym}}{y \leq x} \ \leq\text{-}\mathit{refl}$$

More on Orders

- A partial order is a linear or total order when

$$\forall x, y.\, x \leq y \vee y \leq x$$

Note: no “pure” rule formulation of this disjunction.

- A total order is dense when, in addition

$$\forall x, y.\, x < y \rightarrow \exists z.(x < z \wedge z < y)$$

What does $<$ mean?

Structures for Orders . . .

Give structures for orders that are . . .

1. partial but not total: $\subseteq$-relation;
2. total but not dense: integers with $\leq$;
3. dense: reals with $\leq$.

Example 2: Groups

- Language: Function symbols $\_ \cdot \_$, $\_^{-1}$, e
- A group is a model of

$$\begin{array}{rcll} \forall x, y, z.\, (x \cdot y) \cdot z & = & x \cdot (y \cdot z) & \text{(assoc)} \\ \forall x.\, x \cdot e & = & x & \text{(r-neutr)} \\ \forall x.\, x \cdot x^{-1} & = & e & \text{(r-inv)} \end{array}$$

It is an example of an equational theory.

Theorems: (1) $x^{-1} \cdot x = e$ and (2) $e \cdot x = x$ . . .

Theorem 1

$$\begin{array}{rcll} \forall x, y, z.\, (x \cdot y) \cdot z & = & x \cdot (y \cdot z) & \text{(assoc)} \\ \forall x.\, x \cdot e & = & x & \text{(r-neutr)} \\ \forall x.\, x \cdot x^{-1} & = & e & \text{(r-inv)} \end{array}$$

$$x^{-1} \cdot x = e \quad (1)$$

$$x^{-1} \cdot x = x^{-1} \cdot (x \cdot e) = x^{-1} \cdot (x \cdot (x^{-1} \cdot x^{-1^{-1}})) =$$
$$x^{-1} \cdot ((x \cdot x^{-1}) \cdot x^{-1^{-1}}) = x^{-1} \cdot (e \cdot x^{-1^{-1}}) = \qquad .$$
$$(x^{-1} \cdot e) \cdot x^{-1^{-1}} = x^{-1} \cdot x^{-1^{-1}} = e$$

Theorem 2

$$\begin{array}{lcrr} \forall x, y, z.\, (x \cdot y) \cdot z & = & x \cdot (y \cdot z) & \text{(assoc)} \\ \forall x.\, x \cdot e & = & x & \text{(r-neutr)} \\ \forall x.\, x \cdot x^{-1} & = & e & \text{(r-inv)} \end{array}$$

$$e \cdot x = x \tag{2}$$

$$e \cdot x = (x \cdot x^{-1}) \cdot x = x \cdot (x^{-1} \cdot x) = x \cdot e = x.$$

(Theorem 1)

Lessons Learned from these Examples

Equational proofs are often tricky!

- Equalities used in different directions, “eureka” terms, etc.
- In some cases (the word problem is) decidable.

Equational versus ND Proofs

- Above proofs were of a particular, equational form.
- In Isabelle this is accomplished by term rewriting.

  Term rewriting is a process for replacing equals by equals (see later).
- Alternative is natural deduction:
  - requires explicit proofs using equality rules;
  - tedious in practice. Try it on above examples!

More Detailed Explanations

Theories

Recall our intuitive explanation of theories.

A theory involves certain function and/or predicate symbols for which certain "laws" hold.

Depending on the context, these symbols may co-exist with other symbols.

Technically, the laws are added as rules (in particular, axioms) to the proof system.

A structure in which these rules are true is then called a model of the rules.

Partial Orders

A partial order is a binary relation that is reflexive, transitive, and anti-symmetric: $a \leq b$ and $b \leq a$ implies $a = b$.

A Language Consisting of $\leq$?

$\leq$ is (by convention) a binary infix predicate symbol.

The theory of partial orders involves only this symbol, but that does not mean that there could not be any other symbols in the context.

Antisymmetry and Reflexivity

Note that $\forall x, y.\, x \leq y \wedge y \leq x \leftrightarrow x = y$ encodes both antisymmetry ($\rightarrow$) and reflexivity ($\leftarrow$). Recall that $A \leftrightarrow B$ as shorthand for $A \rightarrow B \wedge B \rightarrow A$.

Transitivity

The axiom $\forall x, y, z.\, x \leq y \wedge y \leq z \rightarrow x \leq z$ encodes transitivity.

Axioms vs. Rules

One can see that using $\rightarrow$-*I* and $\rightarrow$-*E*, one can always convert a proof using the axioms to one using the proper rules.

More generally, an axiom of the form $\forall x_1, \ldots, x_n.\ A_1 \wedge \ldots \wedge A_n \rightarrow B$ can be converted to a rule

$$\frac{A_1 \quad \ldots A_n}{B} \quad .$$

Do it in Isabelle!

Linear and Dense Orders

We define these notions in a usual mathematical terminology.

A partial order $\leq$ is linear or total if for all a, b, either $a \leq b$ or $b \leq a$.

A partial order $\leq$ is dense if for all a, b where $a < b$, there exists a c such that $a < b$ and $b < c$.

“Pure” Rule Formulation

The axiom $\forall x, y.\, x \leq y \vee y \leq x$ cannot be phrased as a proper rule in the style of, for example, the transitivity axiom.

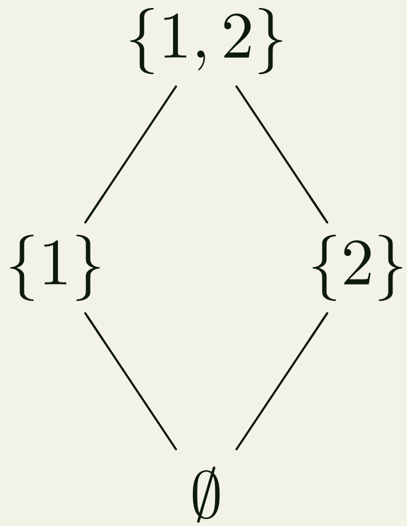
$<$

We use $s < t$ as shorthand for $s \leq t \wedge \neg s = t$.

We say that $<$ is the strict part of the partial order $\leq$.

The $\subseteq$-Relation

The $\subseteq$-relation is partial but not total. As an example, consider the $\subseteq$-relation on the set of subsets of $\{1, 2\}$.



Depicting partial orders by a such a graph is quite common. Here, node a is below node b and connected by an arc if and only if $a < b$ and there exists no c with $a < c < b$.

In this example, we have the partial order

$$\{(\emptyset,\emptyset),(\{1\},\{1\}),(\{1\},\{1\}),(\{1,2\},\{1,2\}),$$
$$(\emptyset,\{1\}),(\emptyset,\{1\}),(\{1\},\{1,2\}),(\{1\},\{1,2\})\}.$$

Group Language

$\_ \cdot \_$ is a binary infix function symbol (in fact, only $\cdot$ is the symbol, but the notation $\_ \cdot \_$ is used to indicate the fact that the symbol stands between its arguments).

$\_^{-1}$ is a unary function symbol written as superscript. Again, the $\_$ is used to indicate where the argument goes.

e is a nullary function symbol (= constant).

Note that groups are very common in mathematics, and many different notations, i.e., function names and fixity (infix, prefix. . .) are used for them.

Group

In general mathematical terminology, a group consists of three function symbols $\_ \cdot \_$, $\_^{-1}$, e, obeying the following laws:

Associativity $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, c,

Right neutral $a \cdot e = a$ for all a,

Right inverse $a \cdot a^{-1} = e$ for all a.

Equational Theory

An equational theory is a set of equations. Each equation is an axiom. Sometimes, each equation is surrounded by several ∀-quantifiers binding all the free variables in the equation, but often the equation is regarded as implicitly universally quantified.

More generally, a conditional equational theory consists of proper rules where the premises are called conditions [Höl90].

Note also that sometimes, one also considers the basic rules of equality as being part of every equational theory. Whenever one has an equational theory, one implies that the basic rules are present; whether or not one assumes that they are formally elements of the equational theory is just a technical detail.

A Model a Group?

A model of the group axioms is a structure in which the group axioms are true.

However, when we say something like, “this model is a group”, then this is a slight abuse of terminology, since there may be other function symbols around that are also interpreted by the structure.

So when we say “this model is a group”, we mean, “this model is a model of the group axioms for function symbols $\_ \cdot \_$, $\_^{-1}$,and e clear from the context”.

“Eureka” terms

By “eureka” terms we mean terms that have to be guessed in order to find a proof. At least at first sight, it seems like these terms simply fall from the sky.

The Greek heureka is 1st person singular perfect of heuriskō, “to find”. It was exclaimed by Archimedes upon discovering how to test the purity of Hiero’s crown.

The Word Problem

The word problem w.r.t. an equational theory (here: the group axioms) is the problem of deciding whether two terms s and t are equal in the theory, that is to say, whether the formula $s = t$ is true in any model of the theory.

Equational Proofs

An equational proof consists simply of a sequence of equations, written as $t_1 = t_2 = \ldots = t_n$, where each t_{i+1} is obtained from t_i by replacing some subterm s with a term s', provided the equality $s = s'$ holds.

This style of proof can be justified by the rules given for equality, in particular the congruences. However, it looks very different from the natural deduction style.

Proof of Theorem 2 by Natural Deduction

$$
\dfrac{
  \dfrac{\boxed{\text{r-neutr}}}{x \cdot e = x}
  \qquad
  \dfrac{
    \dfrac{\text{Theorem 1}}{x^{-1} \cdot x = e}
    \qquad
    \dfrac{
      \dfrac{\boxed{\text{assoc}}}{(x \cdot x^{-1}) \cdot x = x \cdot (x^{-1} \cdot x)}
      \qquad
      \dfrac{\text{cont. below}}{e \cdot x = (x \cdot x^{-1}) \cdot x}
    }{e \cdot x = x \cdot (x^{-1} \cdot x)}
  }{e \cdot x = x \cdot e}
}{e \cdot x = x}
$$

Most steps use the congruence rule $cong_2$.

$$\dfrac{\dfrac{\dfrac{\boxed{\text{r-inv}}}{x \cdot x^{-1} = e}}{e = x \cdot x^{-1}}\,\textit{sym} \qquad \dfrac{}{e \cdot x = e \cdot x}\,\textit{refl}}{e \cdot x = (x \cdot x^{-1}) \cdot x}$$

Proof of Theorem 2 by Natural Deduction, Complete

$$
\dfrac{\dfrac{\boxed{\text{r-neutr}}}{x \cdot e = x} \qquad \dfrac{\dfrac{\text{Theorem 1}}{x^{-1} \cdot x = e} \qquad \dfrac{\dfrac{\boxed{\text{assoc}}}{(x \cdot x^{-1}) \cdot x = x \cdot (x^{-1} \cdot x)} \qquad \dfrac{\dfrac{\dfrac{\boxed{\text{r-inv}}}{(x \cdot x^{-1}) = e}}{e = (x \cdot x^{-1})}\,\textit{sym} \qquad \dfrac{}{e \cdot x = e \cdot x}\,\textit{refl}}{e \cdot x = (x \cdot x^{-1}) \cdot x}}{e \cdot x = x \cdot (x^{-1} \cdot x)}}{e \cdot x = x \cdot e}}{e \cdot x = x}
$$

Each framed box in the derivation tree stands for a sub-tree consisting of a group axiom and possibly several applications of $\forall$-*E*.

References

[Höl90] Steffen Hölldobler. Conditional equational theories and complete sets of transformations. *Theoretical Computer Science*, 75(1&2):85–110, 1990.