Predicate Logic as Working Language

Bruno Buchberger
Research Institute for Symbolic Computation
Johannes Kepler University, Linz, Austria

Version: 2002−05−06

Chapter 4: Exploration Using Quantifier Predicate Logic

■ Quantifier Rules for Proving

■ Existentially Quantified Formulae in the Knowledge Base

■ Rule ("Skolem Constants")

If

$$\underset{\xi,\eta,\ldots}{\exists}\ F$$

is in the knowledge base (where $\xi,\eta,\ldots$ are the only free variables in F)

then you can add

$$F_{\xi,\eta,\ldots\leftarrow x0,y0,\ldots}$$

to the knowledge base, where x0, y0, ... are new object constants (i.e. constants that do neither occur in the knowledge base nor in the goal formula).

(One calls these constants "Skolem constants".)

■ Wording

Application of this rule is often announced in the following way.

"We know

$$\underset{\xi,\eta,\ldots}{\exists}\ F.$$

Therefore we can chose x0, y0, ... such that

$$F_{\xi,\eta,\ldots\leftarrow x0,y0,\ldots}.$$

■ Rule ("Skolem Functions")

If

$$\underset{\alpha,\beta,\ldots}{\forall}\ \underset{\xi,\eta,\ldots}{\exists}\ F$$

is in the knowledge base (where $\alpha,\beta,\xi,\eta,\ldots$ are the only free variables in F)

then you can add

$$F_{\xi,\eta,\ldots\leftarrow x0[\alpha,\beta,\ldots],y0[\alpha,\beta,\ldots],\ldots}$$

to the knowledge base, where x0, y0, ... are new function constants (i.e. function constants that do neither occur in the knowledge base nor in the goal formula).

(One calls these constants "Skolem function constants".)

■ Wording

Application of this rule is often announced in the following way.

"We know

$$\underset{\alpha,\beta,\ldots}{\forall}\ \underset{\xi,\eta,\ldots}{\exists}\ F$$

Therefore we can chose functions x0, y0, ... such that

$$F_{\xi,\eta,\ldots\leftarrow x0[\alpha,\beta,\ldots],y0[\alpha,\beta,\ldots],\ldots}$$

■ Existentially Quantified Formulae as Proof Goals

■ Rule ("Find Appropriate Terms")

If the proof goal is

$$\underset{\xi,\eta,\ldots}{\exists} F$$

(where $\xi,\eta,\ldots$ are the only free variables in F)

then it suffices to find terms s, t, ... such that

$$F_{\xi,\eta,\ldots\leftarrow s,t,\ldots}$$

can be proved.

■ Universally Quantified Formulae in the Knowledge Base

The appropriate rule for formulae of the form

$$\underset{\xi,\eta,\ldots}{\forall} F$$

in the knowledge base was already given in Chapter 3.

■ Universally Quantified Formulae as Proof Goals

The appropriate rule for proof goals of the form

$$\underset{\xi,\eta,\ldots}{\forall} F$$

was already given in Chapter 3.

■ The Interplay Between the Quantifier Rules

The interplay between the proof rules for universally and existentially quantified formulae in the knowledge base and as proof goals is the most important and characteristic aspect of full predicate logic.

Typically, one has proof goals of the form

$$\underset{\alpha}{\forall}\,\underset{\xi}{\exists} F$$

or, as special case, proof goals of the form

$$\underset{\xi}{\exists} F$$

and formulae in the knowledge base of the form

$$\underset{\beta}{\forall}\,\underset{\eta}{\exists} G \qquad (1\,a)$$

or the special form

$$\exists_{\eta} G \qquad (1\,b)$$

In such situations one normally proceeds by taking "an a0 arbitrary but fixed" and tries to find a term s such that

$$F_{\alpha \leftarrow a0, \xi \leftarrow s.}$$

The term s is then typically constructed from the constants available in the knowledge base and, in particular, from the Skolem constant y0 that can be introduced because of (1a) or (1b), i.e. for which

$$F_{\eta \leftarrow y0[\beta]}$$

or

$$F_{\eta \leftarrow y0}$$

holds.

■ Examples

■ The Notion of Limit

■ Definition

In the sequel, some of the variables, like ’x’, range over the real numbers, some others, like ’n’, over the natural numbers, and some others, like ’f’, over sequences of real numbers (i.e. over functions with natural number input and real number output).

Now we define

$$\text{limit}[f, a] \Leftrightarrow \forall_{\epsilon>0} \exists_{N} \forall_{n \geq N} \left(|f[n] - a| < \epsilon \right), \qquad \text{(definition of limit)}$$

$$(f + g)[n] = f[n] + g[n]. \qquad \text{(definition of sequence sum)}$$

■ Available Knowledge

We assume that we have "all" knowledge available on the arithmetical operations, like ’+’, ’−’, ’| |’<’, etc., for example

$$|x + y| \leq |x| + |y|.$$

■ Proposition

We want to prove that

$$\left(\bigwedge \left\{ \begin{matrix} \text{limit}[f, a] \\ \text{limit}[g, b] \end{matrix} \right\} \right) \Rightarrow \text{limit}[f + g, a + b]. \qquad \text{(limit of sum)}$$

■ Proof

Let f, g, a, b be arbitrary but fixed and assume

limit[f, a], (Af)

limit[g, b]. (Ag)

We have to prove

limit[f + g, a + b]. (G)

By (definition of limit), we have to prove

$$\forall_{\epsilon>0}\ \exists_{N}\ \forall_{n\geq N}\ (|(f+g)[n]-(a+b)|<\epsilon).$$

For this, we take ϵ arbitrary but fixed, assume

$\epsilon > 0$, (Aϵ)

and have to find an N0 such that

$$\forall_{n\geq N0}\ (|(f+g)[n]-(a+b)|<\epsilon).$$ (GN0)

Now, by (Af) and (Ag) and (definition of limit), we know that

$$\forall_{\epsilon>0}\ \exists_{N}\ \forall_{n\geq N}\ (|f[n]-a|<\epsilon),$$

$$\forall_{\epsilon>0}\ \exists_{N}\ \forall_{n\geq N}\ (|g[n]-b|<\epsilon),$$

and, hence, by (Aϵ) and (arithmetic), we know in particular that

$$\exists_{N}\ \forall_{n\geq N}\ (|f[n]-a|<\epsilon/2),$$

$$\exists_{N}\ \forall_{n\geq N}\ (|g[n]-b|<\epsilon/2).$$

Hence, we can choose two natural numbers Nf and Ng such that

$$\forall_{n\geq Nf}\ (|f[n]-a|<\epsilon/2),$$ (ANf)

$$\forall_{n\geq Ng}\ (|g[n]-b|<\epsilon/2),$$ (ANg)

We now take

N0 := max[Nf, Ng] (definition of N0)

and try to prove (GN0). In fact, for arbitrary but fixed n with

$n \geq$ N0 (An)

we have

$|(f + g)[n] - (a + b)|$

= by (definition of sequence sum)

$|(f[n] + g[n]) - (a + b)|$

= by (arithmetic)

$|(f[n] - a) + (g[n] - b)|$

$\leq$ by (arithmetic)

$|f[n] - a| + |g[n] - b|$

$<$ by (An), (definition of N0), (ANf), (ANg), (arithmetic)

$\epsilon/2 + \epsilon/2$

$=$ by (arithmetic)

ϵ.

■ Annotated Proof

We now present the same proof with additional annotations and details (in red color) explaining the proof techniques applied.

Let f0, g0, a0, b0 be arbitrary but fixed and assume

limit[f0, a0], (Af)

limit[g0, b0]. (Ag)

We have to prove

limit[f0 + g0, a0 + b0]. (G)

(Note that f0, etc. are new constants and must not be confused with the variables appearing in the (defintion of limit) etc.)

By (definition of limit), using the substitutions

$f \leftarrow f0 + g0,\ a \leftarrow a0 + b0,$

we have to prove

$$\forall_{\epsilon>0}\ \exists_{N}\ \forall_{n\geq N}\ (\,|(f0 + g0)[n] - (a0 + b0)| < \epsilon).$$

For this, we take $\epsilon 0$ arbitrary but fixed, assume

$\epsilon 0 > 0,$ (Aϵ)

and have to find an N0 such that

$$\forall_{n\geq N0}\ (\,|(f0 + g0)[n] - (a0 + b0)| < \epsilon 0).$$ (GN0)

Now, by (Af) and (Ag) and (definition of limit), using the substitutions

$f \leftarrow f0,\ a \leftarrow a0$

we know that

$$\forall_{\epsilon>0}\ \exists_{N}\ \forall_{n\geq N}\ (\,|f0[n] - a0| < \epsilon),$$

and using the substitution

$f \leftarrow g0,\ a \leftarrow b0$

we know that

$$\forall_{\epsilon>0} \exists_{N} \forall_{n\geq N} (|g0[n] - b0| < \epsilon),$$

and, hence, by (Aϵ) and (arithmetic), we know in particular that

$$\exists_{N} \forall_{n\geq N} (|f0[n] - a0| < \epsilon 0/2),$$

$$\exists_{N} \forall_{n\geq N} (|g0[n] - b0| < \epsilon 0/2).$$

(The (arithmetic) used here infers

$$\epsilon 0/2 > 0 \qquad (1)$$

from (Aϵ). Now

$$\forall_{\epsilon>0} \exists_{N} \forall_{n\geq N} (|f0[n] - a0| < \epsilon),$$

which is an abbreviation for

$$\forall_{\epsilon} \left(\epsilon > 0 \Rightarrow \exists_{N} \forall_{n\geq N} (|f0[n] - a0| < \epsilon)\right),$$

implies

$$\epsilon 0/2 > 0 \Rightarrow \exists_{N} \forall_{n\geq N} (|f0[n] - a0| < \epsilon 0/2). \qquad (2)$$

Now, from (1) and (2), by modus ponens, we obtain

$$\exists_{N} \forall_{n\geq N} (|f0[n] - a0| < \epsilon 0/2)$$

)

Hence, we can choose two natural numbers Nf and Ng such that

$$\forall_{n\geq Nf} (|f0[n] - a0| < \epsilon 0/2), \qquad (ANf)$$

$$\forall_{n\geq Ng} (|g0[n] - b0| < \epsilon 0/2). \qquad (ANg)$$

We now take

$$N0 := \max[Nf0, Ng0] \qquad (\text{definition of } N0)$$

and try to prove (GN0). In fact, for arbitrary but fixed n0 with

$$n0 \geq N0 \qquad (An)$$

we have

$$|(f0 + g0)[n0] - (a0 + b0)|$$

$$= \text{by (definition of sequence sum)}$$

$$|(f0[n0] + g0[n0]) - (a0 + b0)|$$

$$= \text{by (arithmetic)}$$

$$|(f0[n0] - a0) + (g0[n0] - b0)|$$

$$\leq \text{by (arithmetic)}$$

$|f0[n0] - a0| + |g0[n0] - b0|$

$\leq$ by (An), (definition of N0), (ANf), (ANg), (arithmetic)

$\epsilon 0 / 2 + \epsilon 0 / 2$

$=$ by (arithmetic)

$\epsilon 0$.

(Each of the steps in the above sequence is a symbolic computation proof step. For example

$$|(f0 + g0)[n] - (a0 + b0)| = |(f[n] + g[n]) - (a + b)|$$

because, by (definition of sequence sum) using the substitutions

$$f \leftarrow f0,\ g \leftarrow g0,\ n \leftarrow n0$$

we have

$$(f0 + g0)[n0] = f0[n0] + g0[n0]$$

and, hence, by replacing

$$(f0 + g0)[n0]$$

by

$$f0[n0] + g0[n0]$$

in

$$|(f0 + g0)[n] - (a0 + b0)|$$

we obtain

$$|(f0 + g0)[n] - (a0 + b0)| = |(f[n] + g[n]) - (a + b)| .$$

)

(From the above chain of proof steps, we can conclude

$$|(f0 + g0)[n0] - (a0 + b0)| < \epsilon$$

in the following way: First,

$$|(f0 + g0)[n0] - (a0 + b0)| = |(f0[n0] + g0[n0]) - (a0 + b0)|$$

and

$$|(f0[n0] + g0[n0]) - (a0 + b0)| = |(f0[n0] - a0) + (g0[n0] - b0)|$$

implies

$$|(f0 + g0)[n0] - (a0 + b0)| = |(f0[n0] - a0) + (g0[n0] - b0)|$$

by the transitivity rule for equality.

Second,

$$|(f0 + g0)[n0] - (a0 + b0)| = |(f0[n0] - a0) + (g0[n0] - b0)|$$

and

$$|(f0[n0] - a0) + (g0[n0] - b0)| \leq |f0[n0] - a0| + |g0[n0] - b0|$$

implies

$$|(f0 + g0)[n0] - (a0 + b0)| \leq |f0[n0] - a0| + |g0[n0] - b0|.$$

This can be concluded from the general proposition

$$(x = y) \wedge (y \leq z) \Rightarrow x \leq z$$

by appropriate substitutions and modus ponens.

Exercise: Prove the above proposition. Which laws for ≤ do you need?)

■ Equivalences and Partitions

■ Overview

We will start from the basic notions of set theory like '∈', '⊂', etc. and assume that their elementary properties are known (i.e. available in the "knowledge base").

In addition, we will assume that the inference rules for the set quantifiers are known: The set quantifiers allow to construct terms of the following form:

$$\{x \mid \Phi\}$$

and

$$\left\{T \underset{x}{\mid} \Phi\right\},$$

where x is a variable,Φ is a formula, and T is a term. We anticipate here the chapter on set theory.

We will define two important notions of elementary set theory

- equivalences and
- partitions

and explore their interrelation.

In the sequel, the variables R, X, P, p, x etc. range over arbitrary objects ("sets").

■ Inference Rules for the Set Quantifiers

First note that

$$\left\{T \underset{x}{\mid} \Phi\right\}$$

is an abbreviation for

$$\left\{y \;\middle|\; \underset{x}{\exists}\, ((y = T) \wedge \Phi)\right\}.$$

If one has to prove that

$$S \in \{x \mid \Phi\},$$

where S is a term, it suffices to prove that

$$\Phi_{x \leftarrow S}\,.$$

Conversely, if

$$S \in \{x \mid \Phi\}$$

is in the knowledge base, one can also add

$$\Phi_{x \leftarrow S}$$

to the knowledge base.

Hence, in order to prove

$$S \in \left\{T \mid \underset{x}{\Phi}\right\}$$

one has to find a term U such that

$$S = T_{x \leftarrow U} \wedge \Phi_{x \leftarrow U}\,.$$

Conversely, if

$$S \in \left\{T \mid \underset{x}{\Phi}\right\}$$

is in the knowledge base, one can introduce a new constant η and add

$$S = T_{x \leftarrow \eta} \wedge \Phi_{x \leftarrow \eta}$$

to the knowledge base.

■ Available Knowledge

We just give the definitions or axioms for some basic notions of set theory. In addition, we assume that all elementary properties of these notions are known.

$$(A = B) \Leftrightarrow \underset{x}{\forall} ((x \in A) \Leftrightarrow (x \in B)) \qquad \text{(set equality)}$$

$$(\langle a, b\rangle = \langle u, v\rangle) \Leftrightarrow ((a = u) \wedge (b = v)) \qquad \text{(pair equality)}$$

$$(A \subseteq B) \Leftrightarrow \underset{x \in A}{\forall} x \in B \qquad (\subseteq :)$$

$$\emptyset = \{x \mid x \neq x\} \qquad (\emptyset :)$$

$$A \bigcup B = \{x \mid x \in A \vee x \in B\} \qquad (\bigcup :)$$

$$A \bigcap B = \{x \mid x \in A \wedge x \in B\} \qquad (\bigcap :)$$

$$U[A] = \left\{x \,\middle|\, \underset{a \in A}{\exists} x \in a\right\} \qquad (U :)$$

$$A \times B = \left\{\langle a, b\rangle \underset{a,b}{\mid} a \in A \wedge b \in B\right\} \qquad (\times :)$$

Here is an example of an elementary property that follows from these definitions and axioms:

$$A = \emptyset \Leftrightarrow \neg \underset{x}{\exists} x \in A.$$

When we use formulae in this knowledge base, we just reference it by the label (set theory).

■ Definition: Equivalences

$$\text{is-equivalence}[R, X] \Leftrightarrow \bigwedge \begin{cases} \text{is-relation}[R, X] \\ \text{is-reflexive}[R, X] \\ \text{is-symmetric}[R] \\ \text{is-transitive}[R] \end{cases} \qquad \text{(is-equivalence :)}$$

$$\text{is-relation}[R, X] \Leftrightarrow (R \subseteq X \times X) \qquad \text{(is-relation :)}$$

$$\text{is-reflexive}[R, X] \Leftrightarrow \underset{x \in X}{\forall} \langle x, x\rangle \in R \qquad \text{(is-reflexive :)}$$

$$\text{is-symmetric}[R] \Leftrightarrow \underset{x,y}{\forall} (\langle x, y\rangle \in R \Rightarrow \langle y, x\rangle \in R) \qquad \text{(is-symmetric :)}$$

$$\text{is-transitive}[R] \Leftrightarrow \underset{x,y,z}{\forall} (\langle x, y\rangle \in R \wedge \langle y, z\rangle \in R \Rightarrow \langle x, z\rangle \in R) \qquad \text{(is-transitive :)}$$

■ Definition: Partitions

$$\text{is-partition}[P, X] \Leftrightarrow \bigwedge \begin{cases} \text{is-subset-set}[P, X] \\ \text{are-all-nonempty}[P] \\ \text{are-all-disjoint}[P] \\ \text{covers}[P, X] \end{cases} \qquad \text{(is-partition :)}$$

$$\text{is-subset-set}[P, X] \Leftrightarrow \underset{p \in P}{\forall} p \subseteq X \qquad \text{(is-subset-set :)}$$

$$\text{are-all-nonempty}[P] \Leftrightarrow \underset{p \in P}{\forall} p \neq \emptyset \qquad \text{(are-all-nonempty :)}$$

$$\text{are-all-disjoint}[P] \Leftrightarrow \underset{p,q \in P}{\forall} (p \neq q \Rightarrow p \bigcap q = \emptyset) \qquad \text{(are-all-disjoint :)}$$

$$\text{covers}[P, X] \Leftrightarrow (U[P] \supseteq X) \qquad \text{(covers :)}$$

■ Definition: Sets Determined by a Relation

$$\text{sets-of-relation}[R, X] = \left\{\text{class}[x, R, X] \underset{x}{\mid} x \in X\right\} \quad \text{(sets-of-relation:)}$$

$$\text{class}[x, R, X] = \left\{y \in X \underset{y}{\mid} \langle y, x\rangle \in R\right\} \quad \text{(class:)}$$

■ Definition: Relation Determined by Sets

$$\text{relation-of-sets}[P, X] = \left\{\langle x, y\rangle \;\Big|\; \underset{x,y\in X}{\;} \exists_{p\in P} (x \in p \wedge y \in p)\right\} \quad \text{(relation-of-sets:)}$$

■ Theorem

We want to prove that

$$\text{is-equivalence}[R, X] \Rightarrow \text{is-partition}[\text{sets-of-relation}[R, X], X] \quad \text{(partition from equivalence)}$$

$$\text{is-partition}[P, X] \Rightarrow \text{is-equivalence}[\text{relation-of-sets}[P, X], X] \quad \text{(equivalence from partition)}$$

$$\text{is-equivalence}[R, X] \Rightarrow (\text{relation-of-sets}[\text{sets-of-relation}[R, X], X] = R) \quad \text{(equivalence of partion of equivalence)}$$

$$\text{is-partition}[P, X] \Rightarrow (\text{sets-of-relation}[\text{relation-of-sets}[P, X], X] = P) \quad \text{(partition of equivalence of partition)}$$

■ Proof of (partition from equivalence)

We take R and X arbitrary but fixed, assume

$$\text{is-equivalence}[R, X]$$

and show

$$\text{is-partition}[\text{sets-of-relation}[R, X], X].$$

For proving this, by (is-partition:), we have to prove

$$\begin{array}{ll} \text{is-subset-set}[P, X], & \text{(SS)} \\ \text{are-all-nonempty}[P], & \text{(NE)} \\ \text{are-all-disjoint}[P], & \text{(DJ)} \\ \text{covers}[P, X]. & \text{(CV)} \end{array}$$

We only show the proof of (DJ). For the other proofs, see the exercises.

▫ Proof of (DJ)

For proving (DJ), by (are-all-disjoint:), we have to prove

$$\underset{p,q\in \text{sets-of-relation}[R,X]}{\forall} (p \neq q \Rightarrow p \cap q = \emptyset).$$

For this, we take p, q arbitrary but fixed, assume

$p \in \text{sets-of-relation}[R, X]$, (p ∈)
$q \in \text{sets-of-relation}[R, X]$, (q ∈)
$p \neq q$, (NE)

and show

$$p \bigcap q = \emptyset.$$

For this, by (set theory), it suffices to prove that

$$\neg \underset{x}{\exists} (x \in p \wedge x \in q).$$

For proving this, we assume that ξ is such that

$$\xi \in p,$$

$$\xi \in q,$$

and show a contradiction. In fact, we show that

$$p = q.$$

By (set theory), for this it is sufficient to show that

$$\underset{x}{\forall} (x \in p \Leftrightarrow x \in q).$$

For this, we take η arbitrary but fixed, assume

$$\eta \in p$$

and show

$$\eta \in q,$$

and we assume

$$\eta \in q$$

and show

$$\eta \in p.$$

We only show one direction. The other direction is analogous.

Now, from (p∈) and (q∈), by (sets-of-relation:), we know that

$$p \in \left\{\text{class}[x, R, X] \underset{x}{\mid} x \in X\right\},$$

$$q \in \left\{\text{class}[x, R, X] \underset{x}{\mid} x \in X\right\}.$$

Because of this we can take α and β such that

$$p = \text{class}[\alpha, R, X],$$

$$q = \text{class}[\beta, R, X].$$

Now, from this and from $\xi \in p$, by (class:), we know that

$\langle \xi, \alpha \rangle \in R$,

$\langle \xi, \beta \rangle \in R$,

$\langle \eta, \alpha \rangle \in R$.

Hence, from is-equivalence[R,X],

$\langle \eta, \beta \rangle \in R$,

i.e., by (class:),

$\eta \in$ class[β, R, X],

i.e.

$\eta \in q$.

■ Proof of (partition from equivalence) with Comments on the Proof Techniques

We take R and X arbitrary but fixed, assume

is-equivalence[R, X]

and show

is-partition[sets-of-relation[R, X], X].

(Note that R and X are now considered to be "new" constants.)

For proving this, by (is-partition:), we have to prove

is-subset-set[P, X],	(SS)
are-all-nonempty[P],	(NE)
are-all-disjoint[P],	(DJ)
covers[P, X].	(CV)

We only show the proof of (DJ). For the other proofs, see the exercises.

▫ Proof of (DJ)

For proving (DJ), by (are-all-disjoint:), we have to prove

$$\forall_{p,q \in \text{sets-of-relation}[R,X]} (p \neq q \Rightarrow p \cap q = \emptyset).$$

For this, we take p, q arbitrary but fixed, assume

$p \in$ sets-of-relation[R, X],	($p \in$)
$q \in$ sets-of-relation[R, X],	($q \in$)
$p \neq q$,	(NE)

and show

$p \cap q = \emptyset$.

For this, by (set theory), it suffices to prove that

$$\neg \underset{x}{\exists} (x \in p \wedge x \in q).$$

(For proving $\neg \underset{x}{\exists}$... we assume $\underset{x}{\exists}$... and show a contradiction. By the assumption $\underset{x}{\exists}$ ..., we are allowed to take an object, call it ξ and assume that ... holds for ξ.)

For proving this, we assume that ξ is such that

$$\xi \in p,$$

$$\xi \in q,$$

and show a contradiction. In fact, we show that

$$p = q.$$

By (set theory), for this it is sufficient to show that

$$\underset{x}{\forall} (x \in p \Leftrightarrow x \in q).$$

For this, we take η arbitrary but fixed, assume

$$\eta \in p$$

and show

$$\eta \in q,$$

and we assume

$$\eta \in q$$

and show

$$\eta \in p.$$

We only show one direction. The other direction is analogous.

Now, from (p∈) and (q∈), by (sets-of-relation:), we know that

$$p \in \left\{\text{class}[x, R, X] \mid \underset{x}{} \; x \in X\right\},$$

$$q \in \left\{\text{class}[x, R, X] \mid \underset{x}{} \; x \in X\right\}.$$

($p \in \left\{\text{class}[x, R, X] \mid \underset{x}{} \; x \in X\right\}$ means that

$$p \in \left\{t \;\middle|\; \underset{x}{\exists} (t = \text{class}[x, R, X] \wedge x \in X)\right\}$$

and this means that p has the property characterizing this set, i.e.

$$\underset{x}{\exists} (p = \text{class}[x, R, X] \wedge x \in X).$$

Hence, we are allowed to take an object, call it α and assume that

$$p = \text{class}[\alpha, R, X],$$

$$\alpha \in X.$$

)

Because of this we can take α and β such that

p = class[α, R, X],

q = class[β, R, X].

Now, from this and from $\xi \in$p, by (class:), we know that

$\langle \xi, \alpha \rangle \in$ R,

$\langle \xi, \beta \rangle \in$ R,

$\langle \eta, \alpha \rangle \in$ R.

Hence, from is-equivalence[R,X],

$\langle \eta, \beta \rangle \in$ R,

i.e., by (class:),

$\eta \in$ class[β, R, X],

i.e.

$\eta \in$ q.

(Here, we may further detail the steps that lead from

$\langle \xi, \alpha \rangle \in$ R,

$\langle \xi, \beta \rangle \in$ R,

$\langle \eta, \alpha \rangle \in$ R,

to

$\langle \eta, \beta \rangle \in$ R.

In fact, from

is-equivalence[R, X],

by (is-equivalence:), we know that

is-symmetric[R, X],

is-transitive[R, X],

and, hence, by (is-symmetric:) and (is-transitive:),

$$\forall_{x,y} (\langle x, y \rangle \in R \Rightarrow \langle y, x \rangle \in R) \qquad (1)$$

$$\forall_{x,y,z} (\langle x, y \rangle \in R \wedge \langle y, z \rangle \in R \Rightarrow \langle x, z \rangle \in R). \qquad (2)$$

Now, from $\langle \xi, \alpha \rangle \in$R, by (1),

$\langle \alpha, \xi \rangle \in$ R.

Now, from $\langle\eta,\alpha\rangle\in$R and $\langle\alpha,\xi\rangle\in$R, by (2),

$$\langle\eta, \xi\rangle \in \text{R}.$$

And now, from $\langle\eta,\xi\rangle\in$R and $\langle\xi,\beta\rangle\in$R, again by (2),

$$\langle\eta, \beta\rangle \in \text{R}.$$

)

■ Structuring Proofs

■ Unfolding Definitions

As shown in the above examples, proofs proceed by "unfolding" the definitions of notions occuring in the goal formula and in the formulae in the knowledge base.

In many proofs, hardly any difficult idea is needed except unfolding the definitions and playing with the constants introduced in the various stages of the proofs for combining suitable terms that fulfill the conditions specified in existentially quantified formulae.

However, proofs of theorems may become quite long. Also, one uses to reference long formulae occurring in proofs by labels. Thus, long proofs may become hard to read because one tends to lose the overview and it is sometimes quite annoying to jump back and forth a couple of pages for finding the formulae referenced in a given proof step. Also, understanding proofs has two very different aspects both of which are equally important:

- understanding the main idea of a proof independent of formal details,
- being able to check the correctness of each step of the proof and the completeness of the proof.

Therefore it is very important to develop techniques for structuring proofs with the goal to invent and understand proofs more easily.

We discuss three techniques for structuring proofs:

- develop the key ideas of proofs in examples, in particular graphic illustrations,
- theory exploration instead of isolated theorem proving,
- introducing only one quantifier at a time,
- "backward proof presentation" versus "forward proof presentation".