Predicate Logic with Equality

Outline

- Rules of Inference for Identity (=)

- Equality & Interpretation Structures

- PVS Commands for Dealing with =

Predicate Logic With Equality

Equality needed to state many useful properties:

E.g. There is one (unique) student with the highest average:

$$(\exists x)(Sx \wedge Hx \wedge (\forall y)(Sy \wedge Hy \rightarrow x = y))$$

E.g. An n element array f of integers does not contain any duplicate elements:

$$(\forall x)(\forall y)(1 \leq x \wedge x \leq n \wedge 1 \leq y \wedge y \leq n$$
$$\wedge x \neq y \rightarrow f(x) \neq f(y))$$

or alternatively

$$(\forall x)(\forall y)(1 \leq x \wedge x \leq n \wedge 1 \leq y \wedge y \leq n$$
$$\wedge f(x) = f(y) \rightarrow x = y)$$

Rules of Inference for Identity (=)

Recall: $\phi[t|x]$, the substitution of t for x in ϕ is the formula obtained by replacing every free occurrence of x by t.

Def: $\phi[x,t|x]$ is the formula obtained by replacing *some* free occurrences of x in ϕ. $\phi[x,t|x]$ is also called a *valid substitution* if no free variable in an occurrence of t is bound in $\phi[x,t|x]$.

Rule I: Rules for Identity

a) Reflexivity of equality: $\vdash (\forall x)(x = x)$

b) Substitution of equal terms:

$$\vdash (\forall x)[(x = t) \to (\phi \leftrightarrow \phi[x,t|x])]$$

c) Symmetry of equality:

$$\vdash (\forall x)(\forall y)(x = y \to y = x)$$

d) Transitivity of equality:

$$\vdash (\forall x)(\forall y)(\forall z)(x = y \wedge y = z \to x = z)$$

Use of Rule I

(c) and (d) can be derived using (a) and (b) (See Rubin p. 230-1)

We can write $t = t$ on any line of a proof. Why?

$$\begin{array}{r|ll} n & \Gamma \ \vdash (\forall x)(x = x) & \text{I - Reflexivity} \\ (n+1) & \qquad t = t & n \text{ US } [t|x] \end{array}$$

Try proof of: $\Gamma \vdash Raa$ for

$\Gamma = \{(\forall x)(Rax \to a = x \vee a = b), (\exists x)(Rax), Sa \wedge \neg Sb\}$

Equality & Interpretation Structures

In interpretation structures = must always be interpreted as the "diagonal relation" if Rule I is to be valid.

$=$	a	b	c	$\dots$
a	T	F	F	F
b	F	T	F	F
c	F	F	T	F
$\vdots$	F	F	F	$\ddots$

In terms of relations = is the subset $\mathbf{U} \times \mathbf{U}$ given by:

$$\{(x, x) | x \in U\}$$

i.e. $a = b$ is true in $\mathbf{S}$ iff $\mathbf{a}$ and $\mathbf{b}$ are the same element.

PVS Commands for Dealing with =

`(EXPAND "t1")` and `(EXPAND "t1" "t2" ...)`

```
equality: THEORY
  BEGIN
  x,y:VAR real
  a:real=1
  f(x,y):real = x+y
  g(x,y):real = x+y

  Ia: THEOREM f(y,a)=g(y,1)
  END equality
```

To prove `THEOREM Ia` you can just use `(SKOLEM!)` to eliminate universal quantifiers and then use variants of the `(EXPAND ...)` command to expand definitions `(EXPAND* "f" "g")` `(EXPAND "a")`.

PVS Commands for Dealing with =

Q: How do you use premises with top level "=" in PVS that are not definitions?

A: The PVS equivalent of Rubin's Rule I part (b) Substitution of Equals: `(REPLACE -n * LR)`.

Equation -n in the premises is of the form

$$t_L = t_R$$

The command makes all valid substitutions of t_R for t_L in all other formulas of the sequent!

Changing the argument LR with RL would replace right-to-left, performing all valid substitutions of t_L for t_R.

Example: Rubin p.244 E11

```
equal11 : THEORY
  BEGIN
  U:TYPE+
  P:PRED[U]
  A,B,C,D:PRED[U]
  x,y : VAR U
  E11: THEOREM (FORALL x,y:A(x)&B(y)=> x=y)
 &(EXISTS x:A(x)&C(x)) & (EXISTS x:B(x)&D(x))
    =>(EXISTS x:C(x)&D(x))
  END equal11
```

Using a combination of (BDDSIMP), (SKOLEM!) and (INST?) reduces `E11` to sequent

```
{-1}  A(x!1)
{-2}  B(x!2)
{-3}  x!1 = x!2
{-4}  C(x!1)
{-5}  D(x!2)
  |-------
{1}   D(x!1)
```

Now you can finish off the proof by replacing `x!1` by `x!2` as follows:

```
Rule? (REPLACE -3 * LR)
Replacing using formula -3,
this simplifies to:
E11 :

{-1}  A(x!2)
[-2]  B(x!2)
[-3]  x!1 = x!2
{-4}  C(x!2)
[-5]  D(x!2)
  |-------
{1}   D(x!2)

which is trivially true.
Q.E.D.
```