Completion Theorem Revisited

Notes on UNITY: 25-90

Jayadev Misra*

Department of Computer Sciences

The University of Texas at Austin

Austin, Texas 78712

(512) 471-9547

misra@cs.utexas.edu

7/26/91

The statement of the completion theorem, given in page 65 of [?], can be written in an equivalent, though simpler, form. For predicates p_i, q_i, where i ranges over a finite set, and predicate r:

$$\frac{\begin{array}{l}(\forall\ i\ ::\ p_i\ \mapsto\ q_i)\\ (\forall\ i\ ::\ q_i\ \ \mathit{unless}\ \ r)\end{array}}{(\wedge\ i\ ::\ p_i)\ \mapsto\ (\wedge\ i\ ::\ q_i)\ \vee\ r)}$$

This version is stated in [?] in page 69 (as formula 1) for two predicate pairs (p, q), (p', q'); its proof is also given there. The proof for the general case, stated above, is similar; apply induction on the number of predicate pairs (p_i, q_i). It is straightforward to see that the above version is equivalent to the completion theorem stated in page 65 of [?].

Bengt Jonsson has observed that the completion theorem does not hold for infinite pairs of predicates (in [?], the theorem is explicitly restricted to finite number of predicate pairs). His counterexample uses the program

```
declare   x : natural
initially x = 0
assign    x := x + 1
```

Let, for all natural i

$p.i\ \equiv\ x = 0$
$q.i\ \equiv\ x > i$

Then,

$(\forall\ i\ ::\ p.i\ \mapsto\ q.i)$ and,
$(\forall\ i\ ::\ q.i$ is stable$)$

If the completion theorem could be applied, we would deduce

*This material is based in part upon work supported by the Texas Advanced Research Program under Grant No. 003658–065 and by the Office of Naval Research Contract N00014-90-J-1640.

$$
\begin{array}{lll}
& (\forall\ i \ :: \ p.i) & \mapsto \ (\forall\ i \ :: \ q.i) \\
\text{i.e.,} & x = 0 & \mapsto \ (\forall\ i \ :: \ x > i)
\end{array}
$$

Using the invariant $(\exists\ j \ :: \ x = j)$ and the substitution axiom

$$x = 0 \ \mapsto \ \mathit{false}$$

Using the impossibility theorem,

$x \neq 0$ is invariant

This invariant contradicts the initial condition.