## Appendix

[*Note: Text enclosed in square brackets and set in this font, is comment, and was put here by the authors. All remaining text has been generated automatically by the PVS system, possibly from what has been keyed-in by the user of the system; no change to the lay-out or type-setting has been made. First, here is the theory (a collection of definitions, called 'sim') that has been fed into the system. We have deleted some definitions, theorems $t_1$, $t_3$ and $t_4$, and some blank lines.*]

sim : THEORY
BEGIN

State : TYPE
PredTrans : TYPE $=$ [pred[State] $\rightarrow$ pred[State]]
StateTuple : TYPE $=$ [State, State]
Relation : TYPE $=$ pred[StateTuple]
$x, y, z$ : VAR State
$p, q$ : VAR pred[State]
$R, S, T$ : VAR Relation
composition$(S, T)$ : Relation $= \lambda\, x, y : \exists\, z : S(x, z) \wedge T(z, y)$
converse$(R)$ : Relation $= \lambda\, x, y : R(y, x)$
subset$(S, T)$ : bool $= \forall\, x, y : S(x, y) \Rightarrow T(x, y)$
stronglySimulates$(R)$ :
[Relation, Relation $\rightarrow$ bool]
$= \lambda\, S, T : R^{\cup}; S; R \subseteq T$
upSimulates$(R)$ :
[Relation, Relation $\rightarrow$ bool]
$= \lambda\, S, T : S; R \subseteq R; T$
[......*And similar definitions for 'weaklySimulates', 'downSimulates'* ...]
total$(R)$ : bool $= \forall\, x : \exists\, y : R(x, y)$
box$(R)$ : PredTrans $= \lambda\, q : \lambda\, x : \forall\, y : R(x, y) \Rightarrow q(y)$
diamond$(R)$ : PredTrans $= \lambda\, q : \lambda\, x : \exists\, y : R(x, y) \wedge q(y)$
leadsto$(p, q)$ : Relation $= \lambda\, x, y : p(x) \Rightarrow q(y)$

$t_2$ :
THEOREM
total$(R) \supset$ upSimulates$(R)([R](p) \leadsto [R](q), p \leadsto q)$

END sim

[*Here is the generated report of the interactive proof process for theorem '$t_2$'. The PVS system performs the bookkeeping, and repeatedly shows the current state within the proof process.* ]

Verbose proof for `t2`.

`t2:`

$$\frac{}{\{1\} \quad (\forall\, (R : \text{Relation}), (p, q : \text{pred[State]}) : \text{total}(R) \supset \text{upSimulates}(R)([R](p) \leadsto [R](q), p \leadsto q))}$$

Rewriting relative to the theories: sim, [... *exactly the same as the preceding formula...*]

Applying auto-rewrites,

`t2:`

$$
\begin{array}{ll}
\hline
\{1\} & (\forall\ (R:\ \text{Relation}), (p, q:\ \text{pred[State]}):\\
& \quad (\forall\ (x:\ \text{State}):\ \exists\ (y:\ \text{State}):\ R(x,y))\\
& \qquad \supset\ \forall\ (x:\ \text{State}), (y:\ \text{State}):\\
& \qquad (\exists\ (z:\ \text{State}):\\
& \qquad\quad ((\forall\ (y:\ \text{State}):\ R(x,y)\ \Rightarrow\ p(y))\ \Rightarrow\ \forall\ (y:\ \text{State}):\ R(z,y)\ \Rightarrow\ q(y))\\
& \qquad\qquad \wedge\ R(z,y))\\
& \qquad\quad \Rightarrow\ \exists\ (z:\ \text{State}):\ R(x,z)\ \wedge\ (p(z)\ \Rightarrow\ q(y)))
\end{array}
$$

Applying (SKOSIMP*), [*that is, Skolemisation and Simplification*]

`t2:`

$$
\begin{array}{ll}
\{-1\} & \forall\ (x:\ \text{State}):\ \exists\ (y:\ \text{State}):\ r'(x,y)\\
\{-2\} & (\forall\ (y:\ \text{State}):\ r'(x',y)\ \Rightarrow\ p'(y))\ \Rightarrow\ \forall\ (y:\ \text{State}):\ r'(z',y)\ \Rightarrow\ q'(y)\\
\{-3\} & r'(z',y')\\
\hline
\{1\} & \exists\ (z:\ \text{State}):\ r'(x',z)\ \wedge\ (p'(z)\ \Rightarrow\ q'(y'))
\end{array}
$$

Splitting conjunctions,

which yields 2 subgoals: [*these are called* `t2.1` *and* `t2.2`, *respectively*]

`t2.1:`

$$
\begin{array}{ll}
\{-1\} & \forall\ (y:\ \text{State}):\ r'(z',y)\ \Rightarrow\ q'(y)\\
\{-2\} & \forall\ (x:\ \text{State}):\ \exists\ (y:\ \text{State}):\ r'(x,y)\\
\{-3\} & r'(z',y')\\
\hline
\{1\} & \exists\ (z:\ \text{State}):\ r'(x',z)\ \wedge\ (p'(z)\ \Rightarrow\ q'(y'))
\end{array}
$$

Instantiating the top quantifier in -2 with the terms: x!1 [‘x!1’ *should have read:* $x'$]

`t2.1:`

$$
\begin{array}{ll}
\{-1\} & \forall\ (y:\ \text{State}):\ r'(z',y)\ \Rightarrow\ q'(y)\\
\{-2\} & \exists\ (y:\ \text{State}):\ r'(x',y)\\
\{-3\} & r'(z',y')\\
\hline
\{1\} & \exists\ (z:\ \text{State}):\ r'(x',z)\ \wedge\ (p'(z)\ \Rightarrow\ q'(y'))
\end{array}
$$

For the top quantifier in -2, we introduce Skolem constants: (y!2) [*should have read:* $y''$]

`t2.1:`

[*...Big formula...*]

[*Followed by two more pages of ‘quantifier instantiation’, ‘propositional simplification’, ‘introduction of Skolem constants’, ‘disjunctive simplification’, finally ending as follows:* ]

This completes the proof of `t2.2`.

Q.E.D.