Algebraic methods in semantics

Edited by Maurice Nivat and John C. Reynolds

Algebraic methods in semantics

Edited by

MAURICE NIVAT

Professor of Information Science, University of Paris VII

JOHN C. REYNOLDS

Professor of Computer and Information Science
Syracuse University, New York

The right of the University of Cambridge to print and sell all manner of books was granted by Henry VIII in 1534. The University has printed and published continuously since 1584.

CAMBRIDGE UNIVERSITY PRESS

Cambridge

London New York New Rochelle
Melbourne Sydney

8

'A la Floyd' induction principles for proving inevitability properties of programs

PATRICK COUSOT, RADHIA COUSOT

1 Introduction 278

2 Programs as transition systems 278

3 Program execution as complete traces 279

4 Inevitability properties of programs 279

5 Floyd's invariant assertions and well-ordered set method for proving total correctness 280

5.1 Partial correctness 280

5.2 Clean behavior (or absence of blocking states) 281

5.3 Termination 281

6 The basic induction principle 282

7 Equivalent induction principles 283

8 Soundness and semantic completeness 289

9 On the use of assertional or relational induction hypotheses 289

10 On nondeterminacy being bounded 291

10.1 m-bounded nondeterminacy 291

10.2 Inevitability can be proved using well-ordering $(\mathbf{m}^\dagger, <)$ 291

10.3 Which ordinals are necessary? 293

11 Decomposition of the verification conditions for partitioned transition systems 294

11.1 States partitioning 294

11.2 Transitions partitioning 295

11.3 Multilevels states and transitions partitioning 297

12 Induction principles for proving inevitability properties of restricted classes of execution traces 298

12.1 Admissible complete traces 298

12.2 Closed sets of admissible complete traces 299

12.3 The transformational approach for proving inevitability properties of non-closed sets of admissible complete traces 300

12.4 The dynamic cutset approach for proving inevitability properties of non-closed sets of admissible complete traces 303

13 Conclusion 310

References 311

1 Introduction

Abstracting from Floyd's [6] invariant assertions and well-ordered set method for proving total correctness of sequential programs, we present induction principles for proving inevitability properties of transition systems. These induction principles are shown to be sound, semantically complete and equivalent. This formalizes Floyd's method independently of any particular programming and assertion language and generalizes it to non-deterministic transition systems (in particular partitioned ones) hence to parallel programs. Considering various classes of bounded nondeterminacy we characterize the corresponding well-founded relations which are necessary and sufficient for completeness.

When the behavior of the transition system is specified by a non-closed set of execution traces (e.g. fair parallelism) Floyd's computational induction method cannot be applied without using auxiliary variables. One approach consists in using Floyd's method for an auxiliary transition relation on states and history variables that exactly generates the original set of traces. Another approach consists in a generalization of the use of loop cutpoints in Floyd's method, in that the choice of the cutpoints (where some termination function has to be decreased) may depend upon computation histories cumulated into auxiliary variables.

2 Programs as transition systems

The operational semantics of a programming language associates a transition system $\langle S, t, \varepsilon \rangle$ with each program of the language.

S is a non-empty class of states.

$t \in (S \times S \to \{\mathrm{tt}, \mathrm{ff}\})$ is a transition relation, understood as a function from pairs of states into truth values (tt is true and ff is false). $t(s, s')$ means that starting in state s and executing one program step can put the program into state s'. For a non-deterministic program, there may be several possible next states s'.

$\varepsilon \in (S \to \{\mathrm{tt}, \mathrm{ff}\})$ characterizes initial states.

3 Program execution as complete traces

Executions of a program $\langle S, t, \varepsilon\rangle$ are modelled by the set $\Sigma\langle S, t, \varepsilon\rangle$ of sequences of states called complete execution traces. A sequence $p = p_0, p_1, p_2, \ldots$ in $\Sigma\langle S, t, \varepsilon\rangle$ represents an execution that starts in state p_0, performs the first program step to reach state p_1, performs the next program step to reach state p_2, etc.

Since execution may not terminate this sequence may be infinite. A finite sequence $p_0, \ldots, p_n$ represents an execution in which the program is blocked in state p_n which has no possible successor state.

More formally,

ω is the set of natural numbers,

0 is the empty set or zero,

If $n \in \omega$ and $n > 0$ then $n = \{0, \ldots, n-1\}$,

If E is a set and $x \in E$ then $E \sim x = \{y \in E : y \neq x\}$.

$\beta \in (S \to \{\mathrm{tt}, \mathrm{ff}\})$

$\beta = \lambda s . [\forall s' \in S . \neg t(s, s')]$ Characterizes blocking states

$\Sigma^0\langle S, t, \varepsilon\rangle = 0$

$\Sigma^n\langle S, t, \varepsilon\rangle = \{p \in (n \to S) : \varepsilon(p_0) \wedge (\forall i \in (n-1) . t(p_i, p_{i+1})) \wedge \beta(p_{n-1})\}$

Finite complete traces of length $n > 0$

(For short, we write p_i instead of $p(i)$).

$\Sigma^\omega\langle S, t, \varepsilon\rangle = \{p \in (\omega \to S) : \varepsilon(p_0) \wedge (\forall i \in \omega . t(p_i, p_{i+1}))\}$

Infinite traces

$$\Sigma\langle S, t, \varepsilon\rangle = \left(\bigcup_{n \in \omega} \Sigma^n\langle S, t, \varepsilon\rangle\right) \cup \Sigma^\omega\langle S, t, \varepsilon\rangle$$

Complete traces

4 Inevitability properties of programs

A property Φ is invariant for a program if it holds for all states which can be reached during program execution (except perhaps for the final states). Absence of global deadlocks for parallel programs is an example of an invariance property.

A property Ψ is inevitable for a program if any program execution eventually leads to a final state satisfying Ψ. Termination, total correctness and absence of individual starvation of parallel processes are inevitability properties of programs.

More formally, if $\Phi, \Psi \in (S \times S \to \{\mathrm{tt}, \mathrm{ff}\})$ are relations between states then Φ is invariant and Ψ inevitable for $\langle S, t, \varepsilon\rangle$ if and only if

$$\forall p \in \Sigma\langle S, t, \varepsilon\rangle . \exists i \in \mathit{Dom}(p) . [\forall j \in i . \Phi(p_0, p_j) \wedge \Psi(p_0, p_i)] \qquad (0)$$

($\mathit{Dom}(p)$ is the domain of function (or relation) p, $\mathit{Rng}(p)$ its range and $\mathit{Fld}(p) = \mathit{Dom}(p) \cup \mathit{Rng}(p)$ its field).

5 Floyd's invariant assertions and well-ordered set method for proving total correctness

Floyd [6] considers programs with states of the form $\langle c, m\rangle$ where $c \in C$ is a control point and $m \in M$ is a memory state (assigning values to variables). Let $\psi \in (\mathrm{M} \times \mathrm{M} \to \{\mathrm{tt}, \mathrm{ff}\})$ be an output specification and $\sigma \in (S \to \{\mathrm{tt}, \mathrm{ff}\})$ be the characteristic function of exit states. Let $\bar{\psi} \in (S \times S \to \{\mathrm{tt}, \mathrm{ff}\})$ be

$$\lambda(\langle \underline{c}, \underline{m}\rangle, \langle \bar{c}, \bar{m}\rangle) . \psi(\underline{m}, \bar{m}).$$

Total correctness is an inevitability property of the form:

$$\forall p \in \Sigma\langle S, t, \varepsilon\rangle . \exists i \in \mathit{Dom}(p) . [(\forall j \in i . \neg\, \sigma(p_j)) \wedge \sigma(p_i) \wedge \bar{\psi}(p_0, p_i)]$$

According to Floyd's method, one proves total correctness by proving first partial correctness, then clean behavior and finally termination.

5.1 *Partial correctness*

Floyd [6]–Naur's [10] method for proving partial correctness consists in first associating an assertion P_c with each control point c of the program, then showing that these assertions are invariant and finally proving that the assertion for final states implies the input-output specification.

The assertion $P_c(\underline{m}, m)$ attached to each program control point $c \in C$ relates the current memory state m to the initial one $\underline{m}$. We take $P_c \in (M \times M \to \{\mathrm{tt}, \mathrm{ff}\})$ (so that using sets (or their characteristic functions) and not formal languages we can get rid of those uncompleteness problems which are related to the unconvenient choice of assertion languages which are too weak for describing these sets).

For proving that these assertions are invariant it must first be shown that the entry assertion holds:

$$\forall \underline{c} \in C, \underline{m} \in M \,.\, [\varepsilon(\langle \underline{c}, \underline{m} \rangle) \Rightarrow P_{\underline{c}}(\underline{m}, \underline{m})]$$

Then for every command of the program it must be verified that if control should enter the command by a control point c with P_c true, then control must leave the command, if at all, by an exit c' with $P_{c'}$ true:

$$\forall c, c' \in C, \underline{m}, m, m' \in M.$$
$$([P_c(\underline{m}, m) \wedge \neg\, \sigma(\langle c, m \rangle) \wedge t(\langle c, m \rangle, \langle c', m' \rangle)] \Rightarrow P_{c'}(\underline{m}, m'))$$

The partial correctness proof ends by showing that if control should reach an exit point of the program then the associated assertion should imply the input–output specification:

$$\forall \bar{c} \in C, \underline{m}, \bar{m} \in M \,.\, ([P_{\bar{c}}(\underline{m}, \bar{m}) \wedge \sigma(\langle \bar{c}, \bar{m} \rangle)] \Rightarrow \psi(\underline{m}, \bar{m}))$$

5.2 *Clean behavior (or absence of blocking states)*

If partial operations are used in a program then a proof of clean behavior must show that their use cannot give rise to undefined effects. If the operational semantics agrees on the convention that states that would lead to such undefined effects are blocking states then the clean behavior proof simply consists in showing that reachable states which are not final must have at least one successor:

$$\forall c \in C, \underline{m}, m \in M.$$
$$([P_c(\underline{m}, m) \wedge \neg\, \sigma(\langle c, m \rangle)] \Rightarrow [\exists c' \in C, m' \in M \,.\, t(\langle c, m \rangle, \langle c', m' \rangle)])$$

5.3 *Termination*

Floyd's method for proving termination consists in first associating with each program control point $c \in C$ a termination function $f_c \in (M \times M \rightarrow Rng(f_c))$.

This termination function is then shown to take its values in a well-ordering $(W, \prec)$, $W \subseteq Rng(f_c)$:

$$\forall c \in C, \underline{m}, m \in M \,.\, ([P_c(\underline{m}, m) \wedge \neg\, \sigma(\langle c, m \rangle)] \Rightarrow f_c(\underline{m}, m) \in W)$$

Finally, termination is proved by showing that after each execution of a command, the current value of the termination function associated with the exit is strictly less than the prior value of the termination function associated with the entrance:

$$\begin{aligned}&\forall c, c' \in C, \underline{m}, m, m' \in M.\\ &\quad([P_c(\underline{m}, m) \wedge \neg\, \sigma(\langle c, m\rangle) \wedge t(\langle c, m\rangle, \langle c', m'\rangle)]\\ &\qquad \Rightarrow [f_{c'}(\underline{m}, m') \prec f_c(\underline{m}, m)])\end{aligned}$$

6 The basic induction principle

Instead of using local assertions P_c attached to program control point $c \in C$, we can use a global invariant I such that (Cousot & Cousot [3]):

$$\begin{aligned}&I \in (S \times S \rightarrow \{\mathrm{tt}, \mathrm{ff}\})\\ &I = \lambda(\langle \underline{c}, \underline{m}\rangle, \langle c, m\rangle).[P_c(\underline{m}, m)]\end{aligned}$$

and a global termination function f such that:

$$\begin{aligned}&f \in (S \times S \rightarrow \bigcup\{Rng(f_c)\colon c \in C\})\\ &f = \lambda(\langle \underline{c}, \underline{m}\rangle, \langle c, m\rangle).[f_c(\underline{m}, m)]\end{aligned}$$

Then it is trivial to check that Floyd's verification conditions (as defined in section 5) are equivalent to the following ones:

Partial correctness:

$$\begin{aligned}&[(\varepsilon(\underline{s}) \Rightarrow I(\underline{s}, \underline{s}))\\ &\wedge\\ &\quad([I(\underline{s}, s) \wedge \neg\, \sigma(s) \wedge t(s, s')] \Rightarrow I(\underline{s}, s'))\\ &\wedge\\ &\quad([I(\underline{s}, \bar{s}) \wedge \sigma(\bar{s})] \Rightarrow \bar{\psi}(\underline{s}, \bar{s}))]\end{aligned}$$

Absence of blocking states:

$$([I(\underline{s}, s) \wedge \neg\, \sigma(s)] \Rightarrow [\exists s' \in S.\, t(s, s')])$$

Termination:

$$\begin{aligned}&[([I(\underline{s}, s) \wedge \neg\, \sigma(s)] \Rightarrow f(\underline{s}, s) \in W)\\ &\wedge\\ &\quad([I(\underline{s}, s) \wedge \neg\, \sigma(s) \wedge t(s, s')] \Rightarrow [f(\underline{s}, s') \prec f(\underline{s}, s)])]\end{aligned}$$

If we now define:

$$\begin{aligned}&\Phi, \Psi \in (S \times S \rightarrow \{\mathrm{tt}, \mathrm{ff}\})\\ &\Phi = \lambda(\underline{s}, s).[\neg\, \sigma(s)]\\ &\Psi = \lambda(\underline{s}, \bar{s}).[\sigma(\bar{s}) \wedge \bar{\psi}(\underline{s}, \bar{s})]\end{aligned}$$

then easy checks show that Floyd's method rests upon the following induction principle:

$$\left.\begin{array}{l}
(\exists I_1 \in (S \times S \to \{\mathrm{tt}, \mathrm{ff}\}),\ f_1 \in (S \times S \to Rng(f_1)),\ W_1 \subseteq Rng(f_1),\\
\quad \prec_1 \in (Rng(f_1) \times Rng(f_1) \to \{\mathrm{tt}, \mathrm{ff}\}).\\
\qquad Wo(W_1, \prec_1)\\
\quad \wedge\\
\quad [\forall \underline{s}, s \in S.\\
\qquad (\varepsilon(\underline{s}) \Rightarrow I_1(\underline{s}, \underline{s}))\\
\qquad \wedge\\
\qquad (I_1(\underline{s}, s) \Rightarrow \quad \Psi(\underline{s}, s)\\
\qquad\qquad\qquad \vee\\
\qquad\qquad\qquad [\Phi(\underline{s}, s) \wedge f_1(\underline{s}, s) \in W_1 \wedge \exists s' \in S.t(s, s') \wedge\\
\qquad\qquad\qquad\quad \forall s' \in S.(t(s, s') \Rightarrow [I_1(\underline{s}, s') \wedge\\
\qquad\qquad\qquad\qquad\qquad f_1(\underline{s}, s') \prec_1 f_1(\underline{s}, s)])])])
\end{array}\right\} \quad (1)$$

Where

$$\begin{array}{rl}
Wo(W, \prec) = & Lo(W, \prec) \wedge Wf(W, \prec)\\
& \text{characterizes well-orderings on } W\\
Lo(W, \prec) = & Spo(W, \prec) \wedge\\
& [\forall x, y \in W.((x \neq y) \Rightarrow (x \prec y \vee y \prec x))]\\
& \text{characterizes linear orderings on } W\\
Wf(W, \prec) = & Rel(W, \prec) \wedge\\
& \forall E \subseteq W.[E \neq 0 \Rightarrow \exists y \in E.(\neg \exists z \in E.z \prec y)]\\
& \text{characterizes well-founded relations on } W\\
Spo(W, \prec) = & Rel(W, \prec) \wedge [\forall x \in W. \neg (x \prec x)] \wedge\\
& [\forall x, y, z \in W.(x \prec y \wedge y \prec z) \Rightarrow (x \prec z)]\\
& \text{characterizes strict partial orders on } W\\
Rel(W, \prec) = & [W \times W \subseteq Dom(\prec) \wedge Rng(\prec) = \{\mathrm{tt}, \mathrm{ff}\}]\\
& \text{characterizes relations on } W
\end{array}$$

7 Equivalent induction principles

A number of variants of the basic induction principle have been used. We now introduce successive transformations which lead to different induction principles. These induction principles will all be shown to be equivalent to the basic one (1).

The range of the termination function f_1 can always be chosen so as to coincide with the well-founded part W_1 of the ordering $\prec_1$:

$$\left.\begin{aligned}
&(\exists I_2 \in (S \times S \to \{\text{tt}, \text{ff}\}),\ f_2 \in (S \times S \to Rng(f_2)),\\
&\quad \prec_2 \in (Rng(f_2) \times Rng(f_2) \to \{\text{tt}, \text{ff}\}).\\
&\quad Wo(Rng(f_2), \prec_2)\\
&\ \wedge\\
&\quad [\forall \underline{s}, s \in S.\\
&\qquad (\varepsilon(\underline{s}) \Rightarrow I_2(\underline{s}, \underline{s}))\\
&\qquad \wedge\\
&\qquad (I_2(\underline{s}, s) \Rightarrow \qquad \Psi(\underline{s}, s)\\
&\qquad\qquad\qquad\qquad \vee\\
&\qquad\qquad\qquad\qquad [\Phi(\underline{s}, s) \wedge \exists s' \in S\,.\,t(s, s') \wedge\\
&\qquad\qquad\qquad\qquad \forall s' \in S\,.\,(t(s, s') \Rightarrow [I_2(\underline{s}, s')\\
&\qquad\qquad\qquad\qquad\qquad \wedge f_2(\underline{s}, s') \prec_2 f_2(\underline{s}, s)]])])
\end{aligned}\right\}\ (2)$$

Proof. (1) ⇒ (2).

Choose

$$\begin{aligned}
&I_2 = \lambda(\underline{s}, s)\,.\,[(f_1(\underline{s}, s) \in W_1 \wedge I_1(\underline{s}, s)) \vee \Psi(\underline{s}, s)]\\
&Rng(f_2) = W_1 \cup \{\perp\} \quad \text{with} \quad \perp \notin W_1\\
&f_2 = \lambda(\underline{s}, s)\,.\,[\textit{if } f_1(\underline{s}, s) \in W_1 \textit{ then } f_1(\underline{s}, s) \textit{ else } \perp]\\
&\prec_2 = \lambda(w', w)\,.\,[(w' = \perp \wedge w \in W_1)\\
&\qquad\qquad\qquad \vee (w' \in W_1 \wedge w \in W_1 \wedge w' \prec_1 w)]
\end{aligned}$$

□

A termination function need not be associated to all program control points but only to loop cut-points:

$$\left.\begin{aligned}
&(\exists K \subseteq S, I_3 \in (K \times K \times S \to (\text{tt}, \text{ff}\}),\ f_3 \in (K \times K \to Rng(f_3)),\\
&\quad \prec_3 \in (Rng(f_3) \times Rng(f_3) \to \{\text{tt}, \text{ff}\}).\\
&\quad Cutset\langle S, t, \varepsilon\rangle(K)\\
&\ \wedge\\
&\quad Wo(Rng(f_3), \prec_3)\\
&\ \wedge\\
&\quad [\forall \underline{s}, s \in K, s' \in S.\\
&\qquad (\varepsilon(\underline{s}) \Rightarrow I_3(\underline{s}, \underline{s}, \underline{s}))\\
&\qquad \wedge\\
&\qquad (I_3(\underline{s}, s, s') \Rightarrow \quad \Psi(\underline{s}, s')\\
&\qquad\qquad\qquad\qquad \vee\\
&\qquad\qquad\qquad\qquad [\Phi(\underline{s}, s') \wedge \exists s'' \in S\,.\,t(s', s'')\\
&\qquad\qquad\qquad\qquad\qquad \wedge \forall s'' \in S\,.\,(t(s', s'') \Rightarrow\\
&\qquad\qquad\qquad\qquad [(s'' \in K \wedge f_3(\underline{s}, s'') \prec_3 f_3(\underline{s}, s)\\
&\qquad\qquad\qquad\qquad\quad \wedge I_3(\underline{s}, s'', s''))\\
&\qquad\qquad\qquad\qquad \vee (s'' \notin K \wedge I_3(\underline{s}, s, s''))]])])
\end{aligned}\right\}\ (3)$$

where

$$\begin{aligned} Cutset\langle S, t, \varepsilon\rangle(K) = [(K \subseteq S) \wedge (\forall \underline{s} \in S\,.\,(\varepsilon(\underline{s}) \Rightarrow \underline{s} \in K)) \wedge \\ \forall p \in \Sigma^{\omega}\langle S, t, \mathrm{tt}\rangle\,.\,\exists i \in \omega\,.\,p_i \in K] \end{aligned}$$

A cutset is a class of states (which, for simplicity, includes initial states and) such that if there were an infinite computation of the program, execution would pass through an infinite sequence of states in the cutset.

Proof. (2) ⇒ (3).

Choose $I_3 = \lambda(\underline{s}, s, s').[I_2(\underline{s}, s') \wedge s = s']$, $Rng(f_3) = Rng(f_2)$, $f_3 = f_2$, $\prec_3 = \prec_2$ and $K = S$. □

The use of well-orderings is not mandatory. Well-founded relations are sufficient (and sometimes more convenient):

$$\left.\begin{aligned} &(\exists I_4 \in (S \times S \to \{\mathrm{tt}, \mathrm{ff}\}),\ f_4 \in (S \times S \to Rng(f_4)), \\ &\quad \prec_4 \in (Rng(f_4) \times Rng(f_4) \to \{\mathrm{tt}, \mathrm{ff}\}). \\ &\quad Wf(Rng(f_4), \prec_4) \\ &\quad \wedge \\ &\quad [\forall \underline{s}, s \in S. \\ &\qquad (\varepsilon(\underline{s}) \Rightarrow I_4(\underline{s}, \underline{s})) \\ &\qquad \wedge \\ &\qquad (I_4(\underline{s}, s) \Rightarrow \quad \Psi(\underline{s}, s) \\ &\qquad\qquad\qquad \vee \\ &\qquad\qquad\qquad [\Phi(\underline{s}, s) \wedge \exists s' \in S\,.\,t(s, s') \wedge \\ &\qquad\qquad\qquad\quad \forall s' \in S\,.\,(t(s, s') \Rightarrow [I_4(\underline{s}, s') \\ &\qquad\qquad\qquad\qquad \wedge\ f_4(\underline{s}, s') \prec_4 f_4(\underline{s}, s)])])]) \end{aligned}\right\} \quad (4)$$

Proof. (3) ⇒ (4).

Let $(Ord, <)$ be the well-ordered class of ordinals. Since $Wo(Rng(f_3), \prec_3)$ implies $Wf(Rng(f_3), \prec_3)$ it is easy to prove by transfinite induction on $\prec_3$ that $\rho = \lambda w.\bigcup\{\rho(w') + 1\colon\ w' \in Rng(f_3) \wedge w' \prec_3 w\}$ (where $\bigcup$ is the supremum of a class of ordinals, $\bigcup 0 = 0$ and $+$ is ordinal addition) is well-defined. Hence we have $\rho \in (Rng(f_3) \to Ord)$ so that we can define:

(i) $\mu \in (S \times S \to Ord)$

$$\begin{aligned} \mu = \lambda(\underline{s}, s').\,&if\ (\forall s \in S\,.\,\neg\, I_3(\underline{s}, s, s') \vee \Psi(\underline{s}, s'))\ then\ 0\ else \\ &\bigcap\{\rho(f_3(\underline{s}, s)) + 1\colon\ s \in S \wedge I_3(\underline{s}, s, s') \wedge \neg\, \Psi(\underline{s}, s')\} \end{aligned}$$

(where $\bigcap$ is the least element of a non-empty class of ordinals)

(ii) $f_4 \in (S \times S \rightarrow Ord \times S)$
$\quad f_4 = \lambda(\underline{s}, s').\langle \mu(\underline{s}, s'), s' \rangle$
(iii) $\ll \in (S \times S \rightarrow \{\text{tt}, \text{ff}\})$ such that $s' \ll s$ iff $[t(s, s') \wedge s' \notin K]$
(iv) $\mathrel{-\!\!\!<}_4 \in (Rng(f_4) \times Rng(f_4) \rightarrow \{\text{tt}, \text{ff}\})$ such that
$\quad \langle w', s' \rangle \mathrel{-\!\!\!<}_4 \langle w, s \rangle$ iff $((w' < w) \vee (w' = w \wedge s' \ll s))$

Since $Wf(Ord, <)$ and $Cutset\langle S, t, \varepsilon \rangle(K)$ implies $Wf(S, \ll)$ we have $Wf(Rng(f_4), \mathrel{-\!\!\!<}_4)$. Choosing $I_4 = \lambda(\underline{s}, s').[\exists s \in S . I_3(\underline{s}, s, s')]$ the proof then essentially consists in showing that:

$$[(\exists s \in S . I_3(\underline{s}, s, s')) \wedge \neg \Psi(\underline{s}, s') \wedge t(s', s'') \wedge s'' \in K] \Rightarrow (\mu(\underline{s}, s') > \mu(\underline{s}, s''))$$

and

$$[(\exists s \in S . I_3(\underline{s}, s, s')) \wedge \neg \Psi(\underline{s}, s') \wedge t(s', s'') \wedge s'' \notin K] \Rightarrow (\mu(\underline{s}, s') \geq \mu(\underline{s}, s'')).$$

□

The use of a termination function can be avoided when using instead an auxiliary variable (w, not appearing as a program variable) which ranges over the field of a well-founded relation and is 'strictly decreased' after each program step:

$$\left.\begin{array}{l}
(\exists W_5, \mathrel{-\!\!\!<}_5 \in (W_5 \times W_5 \rightarrow \{\text{tt}, \text{ff}\}), I_5 \in (W_5 \times S \times S \rightarrow \{\text{tt}, \text{ff}\}). \\
\quad Wf(W_5, \mathrel{-\!\!\!<}_5) \\
\quad \wedge \\
\quad\quad [\forall \underline{s}, s \in S, w \in W_5 . \\
\quad\quad\quad (\varepsilon(\underline{s}) \Rightarrow [\exists \underline{w} \in W_5 . I_5(\underline{w}, \underline{s}, \underline{s})]) \\
\quad\quad\quad \wedge \\
\quad\quad\quad (I_5(w, \underline{s}, s) \Rightarrow \quad \Psi(\underline{s}, s) \\
\quad\quad\quad\quad\quad\quad\quad \vee \\
\quad\quad\quad\quad\quad\quad\quad [\Phi(\underline{s}, s) \wedge \exists s' \in S . t(s, s') \wedge \\
\quad\quad\quad\quad\quad\quad\quad \forall s' \in S . (t(s, s') \Rightarrow [\exists w' \mathrel{-\!\!\!<}_5 w . \\
\quad\quad\quad\quad\quad\quad\quad\quad I_5(w', \underline{s}, s')])])])
\end{array}\right\} \quad (5)$$

Proof. (4) ⇒ (5).

Choose $W_5 = Rng(f_4)$, $\mathrel{-\!\!\!<}_5 = \mathrel{-\!\!\!<}_4$, $I_5 = \lambda(w, \underline{s}, s).[w = f_4(\underline{s}, s) \wedge I_4(\underline{s}, s)]$.

□

Since well-founded relations can be embedded into well-orderings, isomorphism restricted to well-orderings is an equivalence relation and the ordinals pick out exactly one representative from each equivalence class, one can always use the well-ordering $<$ on the class *Ord* of ordinals for inevitability proofs:

$$\left.\begin{array}{l}
(\exists \delta \in Ord,\ I_6 \in (\delta \times S \times S \to \{\mathrm{tt}, \mathrm{ff}\}).\\
\quad [\forall \underline{s}, s, s', \bar{s} \in S,\ \alpha < \delta.\\
\qquad (\varepsilon(\underline{s}) \Rightarrow [\exists \underline{\alpha} < \delta . I_6(\underline{\alpha}, \underline{s}, \underline{s})])\\
\quad\ \wedge\\
\qquad ([I_6(\alpha, \underline{s}, s) \wedge \alpha > 0] \Rightarrow [\Phi(\underline{s}, s) \wedge \exists s' \in S . t(s, s')])\\
\quad\ \wedge\\
\qquad ([I_6(\alpha, \underline{s}, s) \wedge \alpha > 0 \wedge t(s, s')] \Rightarrow [\exists \alpha' < \alpha . I_6(\alpha', \underline{s}, s')])\\
\quad\ \wedge\\
\qquad (I_6(0, \underline{s}, \bar{s}) \Rightarrow \Psi(\underline{s}, \bar{s}))])
\end{array}\right\} \quad (6)$$

Proof. (5) ⇒ (6).

Define a rank function $\rho \in (W_5 \to Ord)$ as:

$$\rho(w) = \bigcap \{\alpha \in Ord\colon \forall w' \in W_5 . [w' \mathrel{-\!\!\!\prec}_5 w \Rightarrow \rho(w') < \alpha]\}$$

(This definition is easily justified, using transfinite induction on $\mathrel{-\!\!\!\prec}_5$, since $\mathrel{-\!\!\!\prec}_5$ is a well-founded relation on W_5).

Observe that $\forall w', w \in W_5 . [(w' \mathrel{-\!\!\!\prec}_5 w) \Rightarrow (\rho(w') < \rho(w))]$.

Define: $\delta = (\bigcup \{\rho(w) + 1\colon w \in W_5\}) + 1$

Choose:

$$\begin{array}{rl}
I_6(\alpha, \underline{s}, s) = (& [\alpha = 0 \wedge \Psi(\underline{s}, s)]\\
 & \quad \vee\\
 & [\exists w \in W_5 . (I_5(w, \underline{s}, s) \wedge \alpha = \rho(w) + 1)]).
\end{array}$$ □

The auxiliary well-founded class (W_1, $Rng(f_2)$, $Rng(f_3)$, $Rng(f_4)$ or W_5) can always be chosen as $(Ord, <)$ but also as $(S \times S, \mathrel{-\!\!\!\prec})$ where $\mathrel{-\!\!\!\prec}$ is some suitable well-founded relation on pairs of states:

$$\left.\begin{array}{l}
(\exists I_7 \in (S \times S \to \{\mathrm{tt}, \mathrm{ff}\}), \mathrel{-\!\!\!\prec}_7 \in ((S \times S) \times (S \times S) \to \{\mathrm{tt}, \mathrm{ff}\}).\\
\quad Wf(S \times S, \mathrel{-\!\!\!\prec}_7)\\
\ \wedge\\
\quad [\forall \underline{s}, s \in S.\\
\qquad (\varepsilon(\underline{s}) \Rightarrow I_7(\underline{s}, \underline{s}))\\
\quad\ \wedge\\
\qquad (I_7(\underline{s}, s) \Rightarrow \quad \Psi(\underline{s}, s)\\
\qquad\qquad\qquad\quad \vee\\
\qquad\qquad\qquad [\Phi(\underline{s}, s) \wedge \exists s' \in S . t(s, s') \wedge\\
\qquad\qquad\qquad \forall s' \in S . (t(s, s') \Rightarrow [I_7(\underline{s}, s') \wedge\\
\qquad\qquad\qquad\qquad\qquad \langle \underline{s}, s' \rangle \mathrel{-\!\!\!\prec}_7 \langle \underline{s}, s \rangle])])])
\end{array}\right\} \quad (7)$$

Proof. (6) ⇒ (7).

Choose

$$I_7(\underline{s}, s) = [\exists\alpha < \delta . I_6(\alpha, \underline{s}, s)]$$

$$\langle \underline{s}', s' \rangle \prec_7 \langle \underline{s}, s \rangle \text{ iff } [\underline{s}' = \underline{s} \wedge \exists\alpha < \delta . I_6(\alpha, \underline{s}, s) \wedge \neg\, \Psi(\underline{s}, s) \wedge \forall\alpha < \delta . ([I_6(\alpha, \underline{s}, s) \wedge \alpha > 0] \Rightarrow \exists\alpha' < \alpha . I_6(\alpha', \underline{s}, s'))]$$

□

The induction principles (1) to (7) are all equivalent in the sense that once a proof has been found which rests upon some induction principle (*i*) involving I_i, $\prec_i, \ldots$ the proof can be rephrased for any other induction principle (*j*), since I_j, $\prec_j, \ldots$ can be derived from I_i, $\prec_i, \ldots$ using the rewriting rules given in the proofs (*i*) ⇒ (*i* **mod**7 + 1) ⇒ ⋯ ⇒ (*j*). The last necessary proof is:

Proof. (7) ⇒ (1).

Choose $W_1 = Rng(f_1) = Ord$, $\prec_1 = <$, $I_1 = I_7$ and $f_1(\underline{s}, s) = \bigcup \{f_1(\underline{s}, s') + 1 : \langle \underline{s}, s^{\circ}) \prec_7 \langle \underline{s}, s \rangle\}$. □

Using a contrapositive version of these induction principles one can prove inevitability properties of programs by *reductio ad absurdum*. For example, the contrapositive version of (6) is:

$$\left.\begin{array}{l}
(\exists\delta \in Ord, I_{\bar{6}} \in (\delta \times S \times S \to \{\mathrm{tt}, \mathrm{ff}\}). \\
\quad [\forall \underline{s}, s, s', \bar{s} \in S, \alpha < \delta . \\
\qquad (\neg\Psi(\underline{s}, \bar{s}) \Rightarrow I_{\bar{6}}(0, \underline{s}, \bar{s})) \\
\quad \wedge \\
\qquad ([\alpha > 0 \wedge (\neg\Phi(\underline{s}, s) \vee \forall s' \in S . \neg\, t(s, s'))] \Rightarrow I_{\bar{6}}(\alpha, \underline{s}, s)) \\
\quad \wedge \\
\qquad ([\alpha > 0 \wedge t(s, s') \wedge \forall\alpha' < \alpha . I_{\bar{6}}(\alpha', \underline{s}, s')] \Rightarrow I_{\bar{6}}(\alpha, \underline{s}, s)) \\
\quad \wedge \\
\qquad (\varepsilon(\underline{s}) \Rightarrow [\exists\underline{\alpha} < \delta . \neg\, I_{\bar{6}}(\underline{\alpha}, \underline{s}, \underline{s})]])])
\end{array}\right\} \quad (\bar{6})$$

Positive and contrapositive versions of the induction principles are obviously equivalent.

Proof

$(i) \Rightarrow (\bar{i})$, $i = 1, \ldots, 7$. Choose $I_{\bar{i}} = \neg\, I_i$.

$(\bar{i}) \Rightarrow (i)$, $i = 1, \ldots, 7$. Choose $I_i = \neg\, I_{\bar{i}}$. □

8 Soundness and semantic completeness

Φ is invariant and Ψ is inevitable for $\langle S, t, \varepsilon\rangle$ if and only if any one of the induction principles is applicable.

Proof. Soundness, (1) $\Rightarrow$ (0).

Assume by *reductio ad absurdum* that there exists $p \in \Sigma\langle S, t, \varepsilon\rangle$ such that $\forall i \in Dom(p).[(\forall j \in i.\Phi(p_0, p_j)) \Rightarrow \neg\Psi(p_0, p_i)]$. Then by induction on i, (1) implies $\forall i \in Dom(p).[(\forall j \in (i+1).\Phi(p_0, p_j)) \wedge I_1(p_0, p_i)]$. If $\exists n \in (\omega \sim 0).p \in \Sigma^n\langle S, t, \varepsilon\rangle$ then $I_1(p_0, p_{n-1})$, $\neg\Psi(p_0, p_{n-1})$ and (1) imply $\exists s' \in S.t(p_{n-1}, s')$, a contradiction. Else, $p \in \Sigma^\omega\langle S, t, \varepsilon\rangle$ so that for all $i \in \omega$ we have $I_1(p_0, p_i)$ and $t(p_i, p_{i+1})$ whence by (1) that $f_1(p_0, p_i) \in W_1$, $f_1(p_0, p_{i+1}) \in W_1$ and $f_1(p_0, p_{i+1}) \prec_1 f_1(p_0, p_i)$ in contradiction with $Wo(W_1, \prec_1)$. □

Proof. Completeness, (0) $\Rightarrow$ (4).

Let us define W and $\prec \in (W \times W \to \{\mathrm{tt}, \mathrm{ff}\})$ such that

(i) $W = \{\langle \underline{s}, s\rangle \in (S \times S)\colon \exists p \in \Sigma\langle S, t, \varepsilon\rangle, i \in Dom(p), k \in i.[\forall j \in i.$
$(\Phi(p_0, p_j) \wedge \neg\Psi(p_0, p_j)) \wedge \Psi(p_0, p_i)$
$\wedge\ \underline{s} = p_0 \wedge s = p_k]\}$

(ii) $\langle \underline{s}', s'\rangle \prec \langle \underline{s}, s\rangle \Leftrightarrow (\exists p \in \Sigma\langle S, t, \varepsilon\rangle, i \in Dom(p), k \in \omega.[\forall j \in i.(\Phi(p_0, p_j)$
$\wedge\ \neg\Psi(p_0, p_j)) \wedge$
$\Psi(p_0, p_i) \wedge \underline{s}' = \underline{s} = p_0 \wedge k + 1 < i \wedge s = p_k$
$\wedge\ s' = p_{k+1}])$

Since $\langle \underline{s}', s'\rangle \prec \langle \underline{s}, s\rangle$ implies $(\underline{s}' = \underline{s} \wedge \Phi(\underline{s}, s) \wedge \neg\Psi(\underline{s}, s) \wedge t(s, s') \wedge \Phi(\underline{s}, s') \wedge \neg\Psi(\underline{s}, s'))$ we have $Wf(W, \prec)$. (Otherwise, there would be a chain $\langle \underline{s}, s_0\rangle \prec \langle \underline{s}, s_1\rangle \prec \ldots$ hence an infinite trace $\underline{s}, p_1, \ldots, p_{k+1}, s_0, s_1, \ldots$ with all states s satisfying $\Phi(\underline{s}, s) \wedge \neg\Psi(\underline{s}, s)$ in contradiction with (0)). Let us now define $Rng(f_4) = W \cup \{\langle \underline{s}, s\rangle\colon\ \Psi(\underline{s}, s)\}$, $f_4 = \lambda(\underline{s}, s).\langle \underline{s}, s\rangle$ and $\langle \underline{s}', s'\rangle \prec_4 \langle \underline{s}, s\rangle$ iff $[(\Psi(\underline{s}', s) \wedge \underline{s}' = \underline{s} \wedge \langle \underline{s}, s\rangle \in W) \vee \langle \underline{s}', s'\rangle \in W \wedge \langle \underline{s}, s\rangle \in W \wedge \langle \underline{s}', s'\rangle \prec \langle \underline{s}, s\rangle)]$. We have $Wf(Rng(f_4), \prec_4)$ so that choosing $I_4 = \lambda(\underline{s}, s).[\langle \underline{s}, s\rangle \in Rng(f_4)]$ the verification conditions of (4) are obviously verified. □

9 On the use of assertional or relational induction hypotheses

If one is only interested in proving that assertions $\Phi = \lambda(\underline{s}, s).\phi(s)$ is invariant and $\Psi = \lambda(\underline{s}, s).\psi(s)$ is inevitable for $\langle S, t, \varepsilon\rangle$, the induction hypothesis I_i in induction principles (i), $i = 1, \ldots, 7$, may be independent of the initial states. In this case it is also complete to choose f_i in (i), $i = 1, \ldots, 4$ as a function not depending upon the initial states. (If moreover $\phi = \lambda s.[\mathrm{tt}]$, $\psi = \lambda s.[\forall s' \in S. \neg t(s, s')]$, $(Rng(f_2), \prec_2) = (Ord, <)$ then induction principle (2) amounts to Lehmann, Pnueli & Stavi's [9] method for proving total convergence).

In general, Ψ is a relation between initial and final states, and in this case the induction hypothesis has to be chosen as a relation (between initial and current states).

Proof. Consider $S = \{0, 1, 2\}$, $\varepsilon = \lambda \underline{s}.[0 \le s \le 1]$, $t = \lambda(s, s').[(s + 1 \in S) \wedge (s' = s + 1)]$, $\Phi = \lambda(\underline{s}, s).\mathrm{tt}$. Then $\Psi = t$ is obviously inevitable. Assume we can find I_1 of the form $\lambda(\underline{s}, s).I(s)$ in (1). Then $\varepsilon(1) \Rightarrow I_1(1, 1)$. Since $\neg\Psi(1, 1)$ and $t(1, 2)$ we have $I_1(1, 2) = I(2) = I_1(0, 2)$. But $\neg\Psi(0, 2)$ and $\forall s' \in S. \neg t(2, s')$, a contradiction. □

The same way, in induction principle (1) it is not complete to choose f as a unary function not depending upon initial states.

Proof. Let us consider $S = \omega$, $\varepsilon = \lambda \underline{s}.\mathrm{tt}$, $t = \lambda(s, s').[s' = s + 1]$ and $\Phi = \lambda(\underline{s}, s).\mathrm{tt}$. Then $\psi = \lambda(\underline{s}, \bar{s}).[\bar{s} = \underline{s} + 2]$ is obviously inevitable. But (1) cannot be applied with f_1 of the form $\lambda(\underline{s}, s).f(s)$. By *reductio ad absurdum* we would have for all $s \in \omega$, $\varepsilon(s) \Rightarrow I_1(s, s)$ so that $I_1(s, s) \wedge \neg\Psi(s, s + 1) \wedge t(s, s + 1)$ would imply $f_1(s, s) \in W_1$ and $f_1(s, s + 1) \prec_1 f_1(s, s)$ that is $f(s) \in W_1$ and $f(s + 1) \prec_1 f(s)$ in contradiction with $W_O(W_1, \prec_1)$. □

If one insists upon using assertional but not relational induction principles, one can use the well-known trick which consists in using auxiliary program variables.

Inevitability properties of $\langle S, t, \varepsilon\rangle$ can always be proved by reasoning upon $\langle S', t', \varepsilon'\rangle$ such that:

$$S' = S \times S$$
$$t' = \lambda(\langle \underline{s}, s\rangle, \langle \underline{s}', s'\rangle).[\underline{s} = \underline{s}' \wedge t(s, s')]$$
$$\varepsilon' = \lambda\langle \underline{s}, s\rangle.[\varepsilon(\underline{s}) \wedge \underline{s} = s]$$

since

$$\forall p \in \Sigma\langle S, t, \varepsilon\rangle.\exists i \in Dom(p).[(\forall j \in i.\Phi(p_0, p_j)) \wedge \Psi(p_0, p_i)]$$
$$\Leftrightarrow \forall p' \in \Sigma\langle S', t', \varepsilon'\rangle.\exists i \in Dom(p').[(\forall j \in i.\Phi(p'_j)) \wedge \Psi(p'_i)]$$

However auxiliary variables are easier to introduce in proofs than in programs (which have a rigid syntax). Moreover this allows reasonings about program proof methods which are language independent.

10 On nondeterminacy being bounded

Floyd [6] noticed that it may be necessary to use other well-orderings than the set $(\omega, <)$ of natural numbers for termination proofs. Dijkstra [5, p. 77] gave the counter-example $S = \mathbb{Z}$, $t = \lambda(x, x').[(x < 0 \wedge x' > 0) \vee (x > 0 \wedge x' = x - 1)]$, $\varepsilon = \lambda \underline{x}.[\underline{x} < 0]$, $\Phi = \lambda(\underline{x}, x).[\mathrm{tt}]$ and $\Psi = \lambda(\underline{x}, \bar{x}).[\bar{x} = 0]$ for which no finite upper bound on the number of transitions required for termination can be given. Dijkstra also proved that when nondeterminacy is bounded then termination can always be proved using $(\omega, <)$. These results are now extended to a more general notion of bounded nondeterminacy.

10.1 **m**-*bounded nondeterminacy*

For any set E, $|E|$ is the cardinality of E.

A transition system $\langle S, t, \varepsilon\rangle$ is said to be *deterministic* if $\forall s \in S.[|\{s' \in S: t(s, s')\}| \leq 1]$ and *nondeterministic* otherwise.

Nondeterminacy is said to be *finite* (Dijkstra says bounded) if $\forall s \in S.\exists n \in \omega.[|\{s' \in S: t(s, s')\}| \leq n]$ or, and this is equivalent, if $\forall s \in S.[|\{s' \in S: t(s , s')\}| < \omega]$ and *infinite* otherwise.

Nondeterminacy is said to be *countable* if $\forall s \in S.[|\{s' \in S: t(s, s')\}| \leq \omega]$ and *uncountable* otherwise.

More generally, if $\mathbf{m} \in Card$ is a cardinal, then we say that the nondeterminacy of a transition system $\langle S, t, \varepsilon\rangle$ is $\mathbf{m}$-*bounded* if $\forall s \in S.[|\{s' \in S: t(s, s')\}| < \mathbf{m}]$.

(In particular nondeterminacy of $\langle S, t, \varepsilon\rangle$ is always $|S|^+$-bounded. Moreover nondeterminacy is countable if and only if it is ω_1-bounded where ω_1 is the least cardinal strictly greater than ω).

10.2 *Inevitability can be proved using well-ordering* $(\mathbf{m}^\dagger, <)$ *when nondeterminacy is* **m**-*bounded*

A cardinal $\mathbf{m}$ is said to be *regular* if for all $\Gamma \subseteq \mathbf{m}$, if $|\Gamma| < \mathbf{m}$ then $\bigcup \Gamma < \mathbf{m}$, otherwise it is said to be *singular*.

For any ordinal α, α^+ is the least cardinal strictly greater than α.

$\mathbf{m}^\dagger = \omega$ if $\mathbf{m} < \omega$,

$\mathbf{m}^\dagger = \mathbf{m}$ if $\mathbf{m}$ is an infinite regular cardinal,

$\mathbf{m}^\dagger = \mathbf{m}^+$ if $\mathbf{m}$ is an infinite singular cardinal.

(For any cardinal $\mathbf{m}$, $\mathbf{m}^\dagger$ is regular (since ω is regular, and assuming the axiom of choice, for any infinite cardinal $\mathbf{m}$, $\mathbf{m}^+$ is regular)).

The following induction principle is sound (since $(8) \Rightarrow (6)$) and complete for proving inevitability properties of transition systems $\langle S, t, \varepsilon\rangle$ with $\mathbf{m}$-bounded nondeterminacy:

$$\left.\begin{array}{ll}
 & (\exists I_8 \in (\mathbf{m}^\dagger \times S \times S \to \{\mathrm{tt}, \mathrm{ff}\}). \\
 & \quad [\forall \underline{s}, s, s', \bar{s} \in S, \alpha < \mathbf{m}^\dagger, \\
(a) & \qquad (\varepsilon(\underline{s}) \Rightarrow [\exists \underline{\alpha} < \mathbf{m}^\dagger . I_8(\underline{\alpha}, \underline{s}, \underline{s})]) \\
 & \quad \wedge \\
(b) & \qquad ([I_8(\alpha, \underline{s}, s) \wedge \alpha > 0] \Rightarrow [\Phi(\underline{s}, s) \wedge \exists s' \in S . t(s, s')]) \\
 & \quad \wedge \\
(c) & \qquad ([I_8(\alpha, \underline{s}, s) \wedge \alpha > 0 \wedge t(s, s')] \Rightarrow [\exists \alpha' < \alpha . I_8(\alpha', \underline{s}, s')]) \\
 & \quad \wedge \\
(d) & \qquad (I_8(0, \underline{s}, \bar{s}) \Rightarrow \Psi(\underline{s}, \bar{s}))])
\end{array}\right\} \quad (8)$$

Proof. $(0) \Rightarrow (8)$.

For all $\underline{s} \in S$, let us define:

(i) $A(\underline{s}) = \{s \in S\colon \exists p \in \Sigma\langle S, t, \varepsilon\rangle . \exists i \in Dom(p) . [p_0 = \underline{s} \wedge (\forall j \in i . \Phi(p_0, p_j)$
$\wedge \neg \Psi(p_0, p_j))$
$\wedge \Psi(p_0, p_i)$
$\wedge \exists k \in i . p_k = s]\}$

($A(\underline{s})$ is the set of those states which are accessible before reaching a final state during some execution starting from $\underline{s}$).

(ii) $F(\underline{s}) = \{\bar{s} \in S\colon \exists p \in \Sigma\langle S, t, \varepsilon\rangle . \exists i \in Dom(p) . [p_0 = \underline{s} \wedge (\forall j \in i . \Phi(p_0, p_j)$
$\wedge \neg \Psi(p_0, p_j))$
$\wedge \Psi(p_0, p_i) \wedge p_i = \bar{s}]\}$

($F(\underline{s})$ is the set of final states which are reached by executions from $\underline{s}$).

(iii) $\mathrel{-\!\!\!\prec}_{\underline{s}} \in (S \times S \to \{\mathrm{tt}, \mathrm{ff}\})$, such that $s' \mathrel{-\!\!\!\prec}_{\underline{s}} s$ iff $[s \in A(\underline{s}) \wedge t(s, s')]$.

Let us first prove that $\forall \underline{s} \in S, Wf(A(\underline{s}) \cup F(\underline{s}), \mathrel{-\!\!\!\prec}_{\underline{s}})$.

If $\neg \varepsilon(\underline{s})$ then $A(\underline{s}) \cup F(\underline{s}) = 0$ and any relation is well-founded on the empty set 0. Otherwise, by *reductio ad absurdum*, assume that there exists an infinite sequence q of states in $A(\underline{s}) \cup F(\underline{s})$ such that for all $i \in \omega$, $q_{i+1} \mathrel{-\!\!\!\prec}_{\underline{s}} q_i$. If $s \in F(\underline{s})$ then $s \notin A(\underline{s})$ so that $\forall s' \in S . \neg(s' \mathrel{-\!\!\!\prec}_{\underline{s}} s)$. Hence no q_i can belong to $F(\underline{s})$. In particular since $q_0 \in A(\underline{s})$ we can assume that $q_0 = \underline{s}$ (otherwise there exists a prefix $\underline{s} = p_0, \ldots, p_k = q_0$ of some trace $p \in \Sigma\langle S, t, \varepsilon\rangle$ with $p_{j+1} \mathrel{-\!\!\!\prec}_{\underline{s}} p_j$ for $j \in k$ which can be adjoined to the left of q).

We have $\varepsilon(q_0)$. Moreover for all $i \in \omega$, $q_{i+1} \prec_{\underline{s}} q_i$ hence $t(q_i, q_{i+1})$. It follows that $q \in \Sigma\langle S, t, \varepsilon\rangle$. But $\forall i \in \omega$, $q_i \in A(q_0)$ whence we have $\Phi(q_0, q_i) \wedge \neg \Psi(q_0, q_i)$ in contradiction with hypothesis (0).

Let us define $\rho_{\underline{s}}(s) = \bigcup \{\rho_{\underline{s}}(s') \dotplus 1 \colon s' \prec_{\underline{s}} s\}$ for $s \in (A(\underline{s}) \cup F(\underline{s}))$. By transfinite induction on the well-founded relation $\prec_{\underline{s}}$, $\rho_{\underline{s}}$ is well defined and $\rho_{\underline{s}} \in (A(\underline{s}) \cup F(\underline{s}) \to \mathit{Ord})$.

Let us now prove that $\forall \underline{s}, s \in S, |\rho_{\underline{s}}(s)| < \mathbf{m}^\dagger$.

The proof is by transfinite induction on the well-founded relation $\prec_{\underline{s}}$. If $\{s' \colon s' \prec_{\underline{s}} s\}$ is empty then $|\rho_{\underline{s}}(s)| = 0 < \omega \leq \mathbf{m}^\dagger$. Otherwise $s' \prec_{\underline{s}} s$ implies $t(s, s')$ so that $|\{s' \colon s' \prec_{\underline{s}} s\}| \leq |\{s' \colon t(s, s')\}| < \mathbf{m} \leq \mathbf{m}^\dagger$ and $|\rho_{\underline{s}}(\underline{s}')| < \mathbf{m}^\dagger$ for $s' \prec_{\underline{s}} s$ by induction hypothesis. Hence either $|\rho_{\underline{s}}(s')| < \omega$ and $|\rho_{\underline{s}}(s') \dotplus 1| = |\rho_{\underline{s}}(s')| \dotplus 1 < \omega \leq \mathbf{m}^\dagger$ or $|\rho_{\underline{s}}(s')| \geq \omega$ in which case $|\rho_{\underline{s}}(s') \dotplus 1| = |\rho_{\underline{s}}(s')| < \mathbf{m}^\dagger$. If $\mathbf{n}$ is an infinite regular cardinal, then for every system $\langle \mathbf{p}_i \colon i \in I\rangle$ of cardinals with $\mathbf{p}_i < \mathbf{n}$ for each $i \in I$ and $|I| < \mathbf{m}$ we have $\bigcup_{i \in I} \mathbf{p}_i < \mathbf{n}$. Hence we conclude that $|\rho_{\underline{s}}(s)| = |\bigcup \{\rho_{\underline{s}}(s') \dotplus 1 \colon s' \prec_{\underline{s}} s\}| < \mathbf{m}^\dagger$.

Finally let I_8 be $\lambda(\alpha, \underline{s}, s).[s \in (A(\underline{s}) \cup F(\underline{s})) \wedge \alpha = \rho_{\underline{s}}(s)]$. We have $I_8 \in (\mathbf{m}^\dagger \times S \times S \to \{\text{tt}, \text{ff}\})$ and the verification conditions of (8) are satisfied:

(*a*) $\varepsilon(\underline{s}) \Rightarrow [\underline{s} \in (A(\underline{s}) \cup F(\underline{s}))] \Rightarrow [\exists \underline{\alpha} < \alpha < \mathbf{m}^\dagger . I_8(\underline{\alpha}, \underline{s}, \underline{s})]$

(*b*) If $[I_8(\alpha, \underline{s}, s) \wedge \alpha > 0]$ then $\bigcup \{\rho_{\underline{s}}(s') \dotplus 1 \colon s' \prec_{\underline{s}} s\} > 0$ so that there exists s' such that $s' \prec_{\underline{s}} s$ (since otherwise $\{\rho_{\underline{s}}(s') \dotplus 1 \colon s' \prec_{\underline{s}} s\}$ would be the empty set 0 and $\bigcup 0 = 0$). This implies $t(s, s')$ and $s \in A(\underline{s})$ hence $\Phi(\underline{s}, s)$.

(*c*) If $[I_8(\alpha, \underline{s}, s) \wedge \alpha > 0 \wedge t(s, s')]$ then $s \in A(\underline{s})$ so that according to hypothesis (0) we must have $s' \in (A(\underline{s}) \cup F(\underline{s}))$ and $s' \prec_{\underline{s}} s$ whence $\rho_{\underline{s}}(s') < \rho_{\underline{s}}(s)$ and $I_8(\rho_{\underline{s}}(s'), \underline{s}, s')$.

(*d*) $I_8(0, \underline{s}, s) \Rightarrow (\rho_{\underline{s}}(s) = 0) \Rightarrow s \in F(\underline{s}) \Rightarrow \Psi(\underline{s}, s)$ □

In particular when nondeterminacy is finite one can choose well-orderings isomorphic with $(\omega, <)$ and when nondeterminacy is countable one can choose well-orderings isomorphic with $(\omega_1, <)$ for proving inevitability properties of transition systems (ω and $\omega_1 = \omega^+$ are regular so that $\omega^\dagger = \omega$ and $\omega_1^\dagger = \omega_1$).

10.3 *Which ordinals are necessary?*

Let $\mathbf{m}$ be a finite or infinite and regular cardinal. Assume that we consider transition systems $\langle S, t, \varepsilon\rangle$ the nondeterminacy of which is $\mathbf{m}$-bounded and we want to prove (0) using induction principle (6) with $\delta < \mathbf{m}^\dagger = \mathbf{m}$. This is not complete.

Proof. This is obvious when $\mathbf{m} = \omega$ and δ is a natural number so that we can assume $\delta \geq \omega$.

Define $S = \{\bot\} \cup (\delta \dot{+} 1)$ where $\bot \notin (\delta \dot{+} 1)$. We have $|S| = 1 + |\delta \dot{+} 1| = |\delta \dot{+} 1| = |\delta| \leq \delta < \mathbf{m}^{\dagger} = \mathbf{m}$. Hence the nondeterminacy of $\langle S, t, \varepsilon \rangle$ is **m**-bounded. Define $t = \lambda(x, x').[(x = \bot \wedge x' \leq \delta) \vee (0 \leq x' < x \leq \delta)]$, $\varepsilon = \lambda \underline{x}.[\underline{x} = \bot]$, $\Phi = \lambda(\underline{x}, x).[\mathrm{tt}]$ and $\Psi = \lambda(\underline{x}, \bar{x}).[\bar{x} = 0]$.

An execution trace $p \in \Sigma\langle S, t, \varepsilon \rangle$ is such that $p_0 = \bot$, $p_i \in Ord$, $i \in (\omega \sim 0)$ and $p_1 > p_2 > \ldots$ so that we must eventually have some $p_i = 0$ since $Wo(Ord, <)$. Hence Ψ is inevitable for $\langle S, t, \varepsilon \rangle$.

However this cannot be proved by (6). Otherwise, having found I_6 satisfying the verification conditions of (6) we could build an infinite strictly decreasing sequence $\gamma_0 > \gamma_1 > \ldots$ of ordinals as follows: set $\gamma_0 = \delta$. Since $\varepsilon(\bot)$ we must have some $\underline{\alpha} < \delta$ such that $I_6(\underline{\alpha}, \bot, \bot)$. Set $\gamma_1 = \underline{\alpha}$. Since $\neg \Psi(\bot, \bot)$ we have $\neg I_6(0, \bot, \bot)$ hence $\gamma_1 > 0$. But $[\gamma_1 > 0 \wedge I_6(\gamma_1, \bot, \bot) \wedge t(\bot, \gamma_0)] \Rightarrow [\exists \alpha < \gamma_1 . I_6(\alpha, \bot, \gamma_0)]$. Set $\gamma_2 = \alpha$. We have $\delta = \gamma_0 > \gamma_1 > \gamma_2$ and $I_6(\gamma_2, \bot, \gamma_0)$. Since $\gamma_0 > 0$ we have $\neg \Psi(\bot, \gamma_0)$ hence $\neg I_6(0, \bot, \gamma_0)$ and $\gamma_2 \neq 0$. Assume we have constructed the sequence up to γ_{j+2} with $\beta \geq \gamma_j > \gamma_{j+1} > \gamma_{j+2} > 0$ and $I_6(\gamma_{j+2}, \bot, \gamma_j)$. According to (6) we have $[\gamma_{j+2} > 0 \wedge I_6(\gamma_{j+2}, \bot, \gamma_j) \wedge t(\gamma_j, \gamma_{j+1})] \Rightarrow [\exists \alpha < \gamma_{j+2} . I_6(\alpha, \bot, \gamma_{j+1})]$. Set $\gamma_{j+3} = \alpha$. Since $\gamma_{j+1} > 0$ we have $\neg \Psi(\bot, \gamma_{j+1})$ so that $\beta \geq \gamma_{j+1} > \gamma_{j+2} > \gamma_{j+3} > 0$ and $I_6(\gamma_{j+3}, \bot, \gamma_{j+1})$. And so, the sequence can be indefinitely extended. □

Although it is restricted to regular cardinal, the result is very general since the first infinite singular cardinal is $\omega_\omega = \bigcup_{i \in \omega} \omega_i$ (which seems to be large enough not to be of genuine importance in computer science).

11 Decomposition of the verification conditions for partitioned transition systems

Conventional program proof methods can be formally constructed by decomposition of the verification conditions involved in the previous induction principles applied to partitioned transition systems [2].

11.1 States partitioning

A states-partitioned transition system is a tuple $\langle S, \mathrm{r}, \pi, t, \varepsilon \rangle$ such that:

(i) $\langle S, t, \varepsilon \rangle$ is a transition system,

(ii) r is a finite non-empty set of block names,

(iii) $\pi \in (\mathrm{r} \to (S \to \{\mathrm{tt}, \mathrm{ff}\}))$ characterizes a cover of the class S of states, i.e. $\forall s \in S . \exists k \in r . \pi_k(s)$.

(A transition system can be partitioned by giving a name to blocks of states playing similar rôles. For instance a π_k, $k \in r$ may characterize states with a given control component).

A proof of invariance of Φ and inevitability of Ψ for a partitioned transition system $\langle S, \mathrm{r}, \pi, t, \varepsilon\rangle$ can be decomposed for each block of the states cover:

$$\left.\begin{array}{l}
(\exists \delta \in Ord, I_9 \in (\mathrm{r} \to (\delta \times S \times S \to \{\mathrm{tt}, \mathrm{ff}\})). \\
\quad [\forall k, l \in \mathrm{r}, \underline{s}, s, s', \bar{s} \in S, \alpha < \delta. \\
\qquad ([\varepsilon(\underline{s}) \wedge \pi_k(\underline{s})] \Rightarrow [\exists \underline{\alpha} < \delta . I_{9k}(\underline{\alpha}, \underline{s}, \underline{s})]) \\
\quad \wedge \\
\qquad ([I_{9k}(\alpha, \underline{s}, s) \wedge \pi_k(s) \wedge \alpha > 0] \Rightarrow [\Phi(\underline{s}, s) \wedge \exists s' \in S . t(s, s')]) \\
\quad \wedge \\
\qquad ([I_{9k}(\alpha, \underline{s}, s) \wedge \pi_k(s) \wedge \alpha > 0 \wedge t(s, s') \wedge \pi_l(s')] \\
\qquad\qquad\qquad\qquad \Rightarrow [\exists \alpha' < \alpha . I_{9l}(\alpha', \underline{s}, s')]) \\
\quad \wedge \\
\qquad ([I_{9k}(0, \underline{s}, \bar{s}) \wedge \pi_k(\bar{s})] \Rightarrow \Psi(\underline{s}, \bar{s}))])
\end{array}\right\} \quad (9.s)$$

Proof

(i) Soundness, (9.s) ⇒ (6).
Choose $\delta_6 = \delta_9$, $I_6(\alpha, \underline{s}, s) = [\exists k \in \mathrm{r} . (\pi_k(s) \wedge I_{9k}(\alpha, \underline{s}, s))]$.

(ii) Semantic completeness, (6) ⇒ (9.s).
Choose $\delta_9 = \delta_6$, $I_{9k}(\alpha, \underline{s}, s) = [\pi_k(s) \wedge I_6(\alpha, \underline{s}, s)]$. □

Example

A version of Floyd's method for programs with states of the form $\langle c, m\rangle$ where $c \in C$ is a control point and $m \in M$ is a memory state can be derived from (9.s) by choosing $r = C$, $\pi_k(\langle c, m\rangle) = [c = k]$, $\Phi(\langle \underline{c}, \underline{m}\rangle, \langle c, m\rangle) = \neg\, \sigma(\langle c, m\rangle)$ and $\Psi(\langle \underline{c}, \underline{m}\rangle, \langle c, m\rangle) = [\sigma(\langle c, m\rangle) \wedge \psi(\underline{m}, m)]$.

To compare with paragraph 5, we can let $P_c(\underline{m}, m)$ be $[\exists \underline{c} \in C . I_{9c}(\langle \underline{c}, \underline{m}\rangle, \langle c, m\rangle)]$. □

11.2 Transitions partitioning

A transitions-partitioned transition system is a tuple $\langle S, n, t, \varepsilon\rangle$ such that:

(i) S is a non-empty class of states,

(ii) n is a non-empty finite set of block names,

(iii) $t \in (\mathrm{n} \to (S \times S \to \{\mathrm{tt}, \mathrm{ff}\}))$ is the transition relation for individual blocks,

(iv) $\varepsilon \in (S \to \{\mathrm{tt}, \mathrm{ff}\})$ characterizes entry states,

and $\langle S, \bigvee_{k \in n} t_k, \varepsilon\rangle$ is a transition system.

(A transition system can be partitioned by giving a name to blocks of transitions playing similar rôles. A t_k, $k \in \mathrm{n}$ can be understood as the transition relation for a command of the program, or for an individual process of a parallel program, etc.).

A proof of invariance of Φ and inevitability of Ψ for a partitioned transition system $\langle S, n, t, \varepsilon\rangle$ can be decomposed into

n independent proofs of invariance and termination for each block of the partition ((9.t)(a, b, c, d))

$n \times (n - 1)$ checks that the proofs for distinct blocks do not interfere ((9.t)(e)),

a proof of absence of blocking states (e.g. *by reductio ad absurdum*) ((9.t)(f)).

$$\left.\begin{array}{ll}
 & \quad(\exists \delta \in Ord,\ I_9 \in (\mathrm{n} \to (\delta \times \mathrm{S} \times \mathrm{S} \to \{\mathrm{tt}, \mathrm{ff}\}))).\\
 & [\forall k \in \mathrm{n}.\\
 & \ (\forall \underline{s}, s, s' \in S, \alpha < \delta.\\
(a) & \qquad (\varepsilon(\underline{s}) \Rightarrow [\exists \underline{\alpha} < \delta . I_{9k}(\underline{\alpha}, \underline{s}, \underline{s})])\\
 & \quad \wedge\\
(b) & \qquad ([I_{9k}(\alpha, \underline{s}, s) \wedge \alpha > 0 \wedge t_k(s, s')] \Rightarrow [\exists \alpha' < \alpha . I_{9k}(\alpha', \underline{s}, s')])\\
 & \quad \wedge\\
(c) & \qquad ([I_{9k}(\alpha, \underline{s}, s) \wedge \alpha > 0] \Rightarrow \Phi(\underline{s}, s))\\
 & \quad \wedge\\
(d) & \qquad (I_{9k}(0, \underline{s}, s) \Rightarrow [\Psi(\underline{s}, s) \vee \beta_k(s)]))]\\
 & \quad \wedge\\
 & \quad [\forall k \in \mathrm{n}, l \in (n \sim k).\\
 & \qquad\qquad (\forall \underline{s}, s, s' \in S, \alpha < \delta, \gamma < \delta.\\
(e) & \qquad\qquad\quad ([I_{9k}(\alpha, \underline{s}, s) \wedge I_{9l}(\gamma, \underline{s}, s) \wedge \gamma > 0 \wedge t_l(s, s')]\\
 & \qquad\qquad\qquad\qquad\qquad \Rightarrow [\exists \alpha' \leq \alpha . I_{9k}(\alpha', \underline{s}, s')]))]\\
 & \quad \wedge\\
 & \quad [\forall \underline{s}, s \in S.\\
(f) & \qquad\qquad ([\forall k \in \mathrm{n} . \beta_k(s) \wedge \neg \Psi(\underline{s}, s)] \Rightarrow [\exists k \in \mathrm{n} . \forall \alpha < \delta .\\
 & \qquad\qquad\qquad\qquad\qquad \neg I_{9k}(\alpha, \underline{s}, s)]])])
\end{array}\right\} \quad (9.\mathrm{t})$$

where

$\beta \in (\mathrm{n} \to (S \to \{\mathrm{tt}, \mathrm{ff}\}))$ characterizes blocking states of process k

$\beta_k = \lambda s . [\forall s' \in S . \neg t_k(s, s')]$

Proof

(i) Soundness, (9.t) implies (5) for $\langle S, \bigvee_{k \in \mathrm{n}} t_k, \varepsilon\rangle$.
Choose $W_5 = (n \to \delta)$, $\gamma' \prec_5 \gamma$ iff $(\exists k \in \mathrm{n}.[(\gamma'_k < \gamma_k) \wedge (\forall j \in (\mathrm{n} \sim k).\ \gamma'_j \leq \gamma_j)])$ and $I_5 = \lambda(\gamma, \underline{s}, s).[\forall k \in \mathrm{n}. I_{9k}(\gamma_k, \underline{s}, s)]$.

(ii) Semantic completeness, (6) for $\langle S, \bigvee_{k \in \mathrm{n}} t_k, \varepsilon\rangle$ implies (9.t).
Choose $I_9 = \lambda k.[\lambda(\alpha, \underline{s}, s).[(I_6(\alpha, \underline{s}, s) \wedge \neg\Psi(\underline{s}, s) \wedge \alpha > 0) \vee (\Psi(\underline{s}, s) \wedge \alpha = 0)]]$. □

Example

A version of the Lamport [8] proof method for parallel programs $[\![P_0 \| \ldots \| P_{n-1}]\!]$ can be derived from (9.t). The transition relation associated with the program is partitioned into n blocks t_k corresponding to each process P_k, hence I_{9k} is a global invariant for process P_k [4]. □

11.3 Multilevels states and transitions partitioning

Partitionings of states and transitions can be combined and applied recursively so as to induce more refined decompositions of the verification conditions. For example, we can consider partitioned transition systems of the form $\langle S, \mathrm{n}, \mathrm{r}, \pi, t, \varepsilon\rangle$ where $t \in (\mathrm{n} \to (S \times S \to \{\mathrm{tt}, \mathrm{ff}\}))$ and $\forall k \in \mathrm{n}$, $\pi_k \in (\mathrm{r}_k \to (S \to \{\mathrm{tt}, \mathrm{ff}\}))$ with $\forall s \in S$, $k \in \mathrm{n}. \exists i \in \mathrm{r}_k. \pi^i_k(s)$. The corresponding induction principle is:

$$\left.\begin{array}{ll}
 & (\exists \delta \in Ord, I.[\forall k \in \mathrm{n}, i \in \mathrm{r}_k. I^i_{9k} \in (\delta \times S \times S \to \{\mathrm{tt}, \mathrm{ff}\})] \wedge \\
 & \quad [\forall k \in n. \\
 & \quad\ (\forall i, i' \in \mathrm{r}_k. \\
 & \quad\ (\forall \underline{s}, \underline{s}, s' \in S, \alpha < \delta. \\
(a) & \qquad ([\varepsilon(\underline{s}) \wedge \pi^i_k(\underline{s})] \Rightarrow [\exists \underline{\alpha} < \delta. I^i_{9k}(\underline{\alpha}, \underline{s}, \underline{s})]) \\
 & \qquad \wedge \\
(b) & \qquad ([I^i_{9k}(\alpha, \underline{s}, s) \wedge \pi^i_k(s) \wedge \alpha > 0 \wedge t_k(s, s') \wedge \pi^{i'}_k(s')] \\
 & \qquad\quad \Rightarrow [\exists \alpha' < \alpha. I^{i'}_{9k}(\alpha', \underline{s}, s')]) \\
 & \qquad \wedge \\
(c) & \qquad ([I^i_{9k}(\alpha, \underline{s}, s) \wedge \pi^i_k(s) \wedge \alpha > 0] \Rightarrow \Phi(\underline{s}, s)) \\
 & \qquad \wedge \\
(d) & \qquad ([I^i_{9k}(0, \underline{s}, s) \wedge \pi^i_k(s)] \Rightarrow [\Psi(\underline{s}, s) \vee \beta_k(s)])))] \\
 & \quad \wedge \\
 & \quad [\forall k \in \mathrm{n}, i, i' \in \mathrm{r}_k, l \in (\mathrm{n} \sim k), j \in \mathrm{r}_l. \\
 & \quad\ (\forall \underline{s}, s, s' \in S, \alpha < \delta, \gamma < \delta. \\
(e) & \qquad ([I^i_{9k}(\alpha, \underline{s}, s) \wedge \pi^i_k(s) \wedge I^j_{9l}(\gamma, \underline{s}, s) \wedge \pi^j_l(s) \\
 & \qquad\quad \wedge t_l(s, s') \wedge \pi^{i'}_k(s')] \Rightarrow [\exists \alpha' \leq \alpha. I^{i'}_{9k}(\alpha', \underline{s}, s')]))] \\
 & \quad \wedge \\
 & \quad [\forall \underline{s}, s \in S. \\
(f) & \qquad ([\forall k \in \mathrm{n}. \beta_k(s) \wedge \neg\Psi(\underline{s}, s)] \Rightarrow [\exists k \in \mathrm{n}. \forall i \in \mathrm{r}_k. \\
 & \qquad\quad (\pi^i_k(s) \Rightarrow \forall \alpha < \delta. \neg I^i_{9k}(\alpha, \underline{s}, s))]])
\end{array}\right\} \text{(9.ts)}$$

Proof

(i) Soundness, (9.ts) $\Rightarrow$ (9.t) for $\langle S, \mathrm{n}, t, \varepsilon \rangle$.
Choose $I_{9tk}(\alpha, \underline{s}, s) = [\exists i \in \mathrm{r}_k . (\pi_k^i(s) \wedge I_{9\mathrm{ts}}{}_k^i(\alpha, \underline{s}, s))]$
(ii) Semantic completeness, (9.t) for $\langle S, \mathrm{n}, t, \varepsilon \rangle \Rightarrow$ (9.ts).
Choose $I_{9\mathrm{ts}}{}_k^i(\alpha, \underline{s}, s) = [\pi_k^i(s) \wedge I_{9tk}(\alpha, \underline{s}, s)]$ □

Example

A version of the Lamport [7] and Owicki & Gries [11] proof method for parallel programs $[\![P_0 || \ldots || P_{n-1}]\!]$ can be derived from (9.ts). The transition relation associated with the program is partitioned into n blocks t_k corresponding to each process P_k, r_k is the set of control points of process k and π_k^i holds for states such that their control component for process k is equal to i. It follows that I_{9k}^{i} can be attached to point i of process k. Moreover, executing an atomic action of process l cannot modify control in process k so that the only case to be considered in (9.ts)(e) is $i = i'$ [3]. □

12 Induction principles for proving inevitability properties of restricted classes of execution traces

12.1 Admissible complete traces

Given a set S of states for a program P, computations of P can be specified by a set $\theta(S)$ of complete traces on S or by a transition relation on states (in which case the corresponding set of complete traces is $\Sigma\langle S, t, \varepsilon \rangle$ where $\varepsilon = \lambda \underline{s} . \mathrm{tt}$).

The advantage of using a transition relation on states is that inevitability proofs can be done by computational induction. The disadvantage is that the corresponding set of complete traces $\Sigma\langle S, t, \varepsilon \rangle$ may be too large (e.g. when taking fairness requirements into account).

On the contrary any program behaviour can be specified by a set $\theta(S)$ of complete traces on S. However there may be no transition relation on S generating exactly $\theta(S)$.

Therefore we choose to represent (somewhat redundantly) program behaviors by a partitioned transition system $\langle S, \mathrm{n}, t, \varepsilon \rangle$ and a set $\theta\langle S, \mathrm{n}, t, \varepsilon \rangle \subseteq \Gamma(\Sigma\langle S, \bigvee_{k \in \mathrm{n}} t_k, \varepsilon \rangle)$ of admissible complete traces ($\Gamma(\Sigma\langle S, \bigvee_{k \in \mathrm{n}} t_k, \varepsilon \rangle)$ is the prefix closure of $\Sigma\langle S, \bigvee_{k \in \mathrm{n}} t_k, \varepsilon \rangle$. More precisely, let $\Sigma^*\langle S\rangle$ be $\bigcup_{m\in\omega}(m \to S)$, $\Sigma^\omega\langle S\rangle$ be $(\omega \to S)$ and $\Sigma\langle S\rangle$ be $\Sigma^*\langle S\rangle \cup \Sigma^\omega\langle S\rangle$. When $p \in \Sigma\langle S\rangle$ and $m \in (Dom(p) \sim 0)$, $p[m] = p_0 \ldots p_{m-1}$ is the prefix of length m of p. Then when $E \subseteq \Sigma\langle S\rangle$, $\Gamma(E) = E \cup \{p[m] \colon p \in E \wedge m \in (Dom(p) \sim 0)\}$).

Example

An execution trace of a partitioned transition system is said to be *weakly fair* if it is finite or if it is infinite but there is no process which beyond a certain point, is continuously enabled but never activated:

$$\theta wf\langle S, \mathrm{n}, t, \varepsilon\rangle = \bigcup_{m\in\omega} \Sigma^m \langle S, \bigvee_{k\in n} t_k, \varepsilon\rangle$$
$$\cup$$
$$\{p \in \Sigma^\omega\langle S, \bigvee_{k\in n} t_k, \varepsilon\rangle \colon \neg[\exists k \in n . \exists i \in \omega . \forall j \geq i .$$
$$(\neg\, \beta_k(p_j) \wedge \neg\, t_k(p_j, p_{j+1}))]\} \quad \square$$

12.2 Closed sets of admissible complete traces

When $p \in \Sigma^*\langle S\rangle$, $s \in S$, $q \in \Sigma\langle S\rangle$, pq (respectively psq) is the concatenation of p and q (respectively p, s and q).

We say that $\theta \subseteq \Sigma\langle S\rangle$ is closed iff:

$$(\{\forall p_1, p_2 \in \Sigma^*\langle S\rangle, s \in S, q_1, q_2 \in \Sigma\langle S\rangle . (p_1 s q_1 \in \theta \wedge p_2 s q_2 \in \theta)$$
$$\Rightarrow (p_1 s q_2 \in \theta)]$$
$$\wedge [\forall p \in \Sigma^\omega\langle S\rangle . (\forall m \in (\omega \sim 0) . \exists q \in \Sigma\langle S\rangle . p[m]q \in \theta) \Rightarrow (p \in \theta)])$$

Counter-example.

Assume $S = \{a, b\}$, $n = 2$, $t_0 = \lambda(s, s') . [(s = a) \wedge (s' = b)]$, $t_1 = \lambda(s, s')$. $[s = s' = a]$, $\varepsilon = \lambda \underline{s} . [\underline{s} = a]$. $\theta wf\langle S, \mathrm{n}, t, \varepsilon\rangle$ is not closed because it contains all finite traces of the form $a \ldots ab$ but not the infinite trace $a \ldots a \ldots$. □

A set θ of complete traces on a set S of states can be exactly generated by a transition relation on S if and only if it is closed:

$$\forall S . \forall \theta \subseteq \Sigma\langle S\rangle . [(\exists t \in (S \times S \to \{\mathrm{tt}, \mathrm{ff}\}), \varepsilon \in (S \to \{\mathrm{tt}, \mathrm{ff}\}) .$$
$$\Sigma\langle S, t, \varepsilon\rangle = \theta) \Leftrightarrow (\theta \text{ is closed})]$$

Proof

$\Rightarrow$ is trivial. For $\Leftarrow$ we define $\varepsilon = \lambda \underline{s}.[\exists p \in \theta . p_0 = \underline{s}]$ and $t = \lambda(s, s').[\exists p \in \theta, i \in Dom(p). i > 0 \wedge s = p_{i-1} \wedge s' = p_i]$ so that obviously $\theta \subseteq \Sigma\langle S, t, \varepsilon\rangle$. Moreover if $p \in \Sigma\langle S, t, \varepsilon\rangle$ then $\varepsilon(p_0)$ implies $p_0 q^0 \in \theta$ for some $q^0 \in \Sigma\langle S\rangle$. Assume, by induction hypothesis, that $p_0 \dots p_{i-1} q^{i-1} \in \theta$ for some $q^{i-1} \in \Sigma\langle S\rangle$ and $i \in Dom(p)$. Then by definition of $\Sigma\langle S, t, \varepsilon\rangle$ and t there exist $r \in \Sigma^*\langle S\rangle, q^i \in \Sigma\langle S\rangle$ such that $r p_{i-1} p_i q^i \in \theta$ so that $p_0 \dots p_{i-1} p_i q^i \in \theta$ since θ is closed. If $p \in \Sigma^m\langle S\rangle$ then in particular $p_0 \dots p_{m-1} q^{m-1} \in \theta$ and q^{m-1} is the empty trace (otherwise p_{m-1} could not be a blocking state since $t(p_{m-1}, q_0^{m-1})$) so that $p \in \theta$. Else $p \in \Sigma^\omega\langle S\rangle$ and $(\forall m \in (\omega \sim 0). \exists q \in \Sigma\langle S\rangle . p[m] q \in \theta)$ so that $p \in \theta$ because θ is closed. □

When considering closed sets of admissible traces $\theta\langle S, \mathrm{n}, t, \varepsilon\rangle$, any induction principle (1) to (9) can be used for some adequate transition relation on S.

12.3 *The transformational approach for proving inevitability properties of non-closed sets of admissible complete traces*

If we want to use induction principles (1) to (9) in order to prove inevitability properties for a non-closed set of admissible traces then we must abandon the idea of using a transition relation on S. However we can use any auxiliary transition system $\langle S^\sharp, t^\sharp, \varepsilon^\sharp\rangle$ which, up to some correspondence $\rho^\sharp \in (S^\sharp \to S)$, exactly generates the admissible traces:

$\rho^\sharp(\Sigma\langle S^\sharp, t^\sharp, \varepsilon^\sharp\rangle) = \theta\langle S, \mathrm{n}, t, \varepsilon\rangle$

where

$\rho^\sharp(E) = \{\rho^\sharp(x): x \in E\}$ when E is a set and
$\rho^\sharp(f) = \lambda x . \rho^\sharp(f(x))$ when f is a map

It is clear that in general $\langle S^\sharp, t^\sharp, \varepsilon^\sharp\rangle$ is a mathematical object which may not be computable (think of the case when $\theta\langle S, \mathrm{n}, t, \varepsilon\rangle = \bigcup_{m \in \omega} \Sigma^m\langle S, \bigvee_{k \in \mathrm{n}} t_k, \varepsilon\rangle$). However from a theoretical point of view, the auxiliary transition system can always be naïvely defined as:

$S^\sharp = \theta\langle S, \mathrm{n}, t, \varepsilon\rangle \times \omega$
$t^\sharp = \lambda(\langle p, i\rangle, \langle p', i'\rangle).[(i+1) \in Dom(p) \wedge p' = p \wedge i' = i + 1]$
$\varepsilon^\sharp = \lambda\langle p, i\rangle.[i = 0]$

with

$\rho^\sharp = \lambda\langle p, i\rangle . p_i$

Moreover we are interested by admissible traces that, in practice, have to be realized by machines so that more constructive definitions of $\langle S^{\sharp}, t^{\sharp}, \varepsilon^{\sharp}\rangle$ for specifying $\theta\langle S, \mathrm{n}, t, \varepsilon\rangle$ do exist.

Example

Weak fairness can be guaranteed by scheduling execution of individual processes. There are many such schedulers [1, 12, 13]; here is another one:

$$\begin{aligned}
S^{\boxslash} &= (\mathrm{n} \to \omega) \times S \\
t^{\boxslash} &= \lambda(\langle m, s\rangle, \langle m', s'\rangle).[\exists k \in \mathrm{n}.t_k(s, s') \wedge ([m_k > 0 \wedge m'_k < m_k \\
&\qquad \wedge \forall j \in (\mathrm{n} \sim k).(m'_j = m_j)] \\
&\qquad \vee [\forall j \in \mathrm{n}.((\beta_j(s) \vee m_j = 0) \\
&\qquad \wedge m'_j > 0)])] \\
\varepsilon^{\boxslash} &= \lambda\langle m, s\rangle.\varepsilon(s)
\end{aligned}$$

with

$\rho^{\boxslash} = \lambda\langle m, s\rangle.s$

(The scheduler organizes an execution into rounds. During a round all continuously enabled processes will be actived at least once but finitely often. From state $\langle m, s\rangle$ on, a process t_k, $k \in \mathrm{n}$ can be activated at most m_k times within the current round. A new round can begin in state s, if all unblocked processes have been activated at least once and at most as many times as predicted at the begining of the round.)

Proof. $\rho^{\boxslash}(\Sigma\langle S^{\boxslash}, t^{\boxslash}, \varepsilon^{\boxslash}\rangle) = \theta wf\langle S, \mathrm{n}, t, \varepsilon\rangle$.

If $p^{\boxslash} \in \Sigma\langle S^{\boxslash}, t^{\boxslash}, \varepsilon^{\boxslash}\rangle$ then $\rho^{\boxslash}(p^{\boxslash}) \in \theta wf\langle S, \mathrm{n}, t, \varepsilon\rangle$. This is obvious if $p^{\boxslash}$ is finite. Otherwise let $m \in (\omega \to (\mathrm{n} \to \omega))$ and $p \in (\omega \to S)$ be such that $\forall i \in \omega.(p_i^{\boxslash} = \langle m_i, p_i\rangle)$. Assume that $p = \rho^{\boxslash}(p^{\boxslash}) \in \Sigma^{\omega}\langle S, \bigvee_{k\in\mathrm{n}} t_k, \varepsilon\rangle$ is unfair, so that $\exists k \in n.\exists i \in \omega.\forall j \geq i.(\neg\beta_k(p_j) \wedge \neg t_k(p_j, p_{j+1}))$. Within a round $\sum_{k\in\mathrm{n}} m_{jk}$ strictly decreases at each step, so that no round can be infinite. In particular the round to which i belongs must finish at $i' \geq i$. At the beginning of the next round we have $m_{(i'+1)k} > 0$ and the m_{jk} are not modified during this round which must eventually end at $i'' > i$. Then we have $\neg\beta_k(p_{i''}) \wedge m_{i''k} = m_{(i'+1)k} > 0$, a contradiction.

If $p \in \theta wf\langle S, \mathrm{n}, t, \varepsilon\rangle$ we construct $m \in (Dom(p) \to (\mathrm{n} \to \omega))$ such that $p^{\boxslash}$ defined by $(Dom(p^{\boxslash}) = Dom(p) \wedge \forall i \in Dom(p).(p_i^{\boxslash} = \langle m_i, p_i\rangle))$ belongs to $\Sigma\langle S^{\boxslash}, t^{\boxslash}, \varepsilon^{\boxslash}\rangle$.

If $Dom(p) = d \in (\omega - \{0, 1\})$ then $m_i = \lambda k.\sum_{j=1}^{d-2}$ *if* $t_k(p_j, p_{j+1})$ *then* 1 *else* 0.

If $Dom(p) = \omega$ then thanks to the weak fairness hypothesis, we can inductively define $\gamma \in (\omega \to \omega)$ by $\gamma_0 = 0$ and $\gamma_{i+1} = min\{j \in \omega : \forall k \in n.[(\forall l \geq \gamma_i . \beta_k(p_1)) \vee (\exists l \in \omega . \gamma_i \leq l < j \wedge t_k(p_l, p_{l+1}))]\}$ so that all processes not continuously disabled after γ_i are activated at least once between γ_i and γ_{i+1}. Define $\eta \in (\omega \to \omega)$ such that η_i is the γ_{j+1} such that $\gamma_j \leq i < \gamma_{j+1}$. Then we let $m_i = \lambda k . \sum_{j=i}^{\eta_i} \mathit{if}\ t_k(p_j, p_{j+1})\ \mathit{then}\ 1\ \mathit{else}\ 0$.

□

Whenever $\theta\langle S, \mathrm{n}, t, \varepsilon\rangle = \rho^{\#}(\Sigma\langle S^{\#}, t^{\#}, \varepsilon^{\#}\rangle)$, inevitability properties for admissible traces of $\langle S, \mathrm{n}, t, \varepsilon\rangle$:

$$\forall p \in \theta\langle S, \mathrm{n}, t, \varepsilon\rangle . \exists i \in Dom(p) . [(\forall j \in i . \Phi(p_0, p_j)) \wedge \Psi(p_0, p_i)] \tag{10}$$

can be proved by proving similar inevitability properties for all complete traces of $\langle S^{\#}, t^{\#}, \varepsilon^{\#}\rangle$:

$$\forall p \in \Sigma\langle S^{\#}, t^{\#}, \varepsilon^{\#}\rangle . \exists i \in Dom(p) . [(\forall j \in i . \Phi(\rho^{\#}(p_0), \rho^{\#}(p_j))) \wedge \Psi(\rho^{\#}(p_0), \rho^{\#}(p_i))] \tag{11}$$

Such a proof can be done by application of any one of the induction principles (1) to (9) to $\langle S^{\#}, t^{\#}, \varepsilon^{\#}\rangle$.

When $S^{\#}$, $t^{\#}$ and $\varepsilon^{\#}$ are defined in term of S, n, t, ε (and auxiliary domains), we can substitute these definitions for $S^{\#}, t^{\#}, \varepsilon^{\#}$ in the verification conditions dealing with $\langle S^{\#}, t^{\#}, \varepsilon^{\#}\rangle$ so as to obtain equivalent verification conditions dealing with the original $\langle S, \mathrm{n}, t, \varepsilon\rangle$ (and auxiliary variables). Then, by construction, the derived induction principle is sound and semantically complete.

Example

Using induction principle (6) for $\langle S^{\boxslash}, t^{\boxslash}, \varepsilon^{\boxslash}\rangle$ and letting $I_6(\alpha, \langle \underline{m}, \underline{s}\rangle, \langle m, s\rangle)$ be $I_{12}(\alpha, m, \underline{s}, s)$ we obtain an induction principle for proving inevitability properties of $\langle S, \mathrm{n}, t, \varepsilon\rangle$ under weak fairness hypothesis

$$\left.\begin{aligned}
&(\exists \delta \in Ord, I_{12}(\delta \times (\mathrm{n} \to \omega) \times S \times S \to \{\mathrm{tt}, \mathrm{ff}\}).\\
&\quad [\forall \underline{s}, s, s', \bar{s} \in S, \alpha < \delta, \underline{m}, m, m' \in (\mathrm{n} \to \omega), k \in \mathrm{n}.\\
&\qquad (\varepsilon(\underline{s}) \Rightarrow [\exists \underline{\alpha} < \delta . I_{12}(\underline{\alpha}, \underline{m}, \underline{s}, \underline{s})])\\
&\quad \wedge\\
&\qquad ([I_{12}(\alpha, m, \underline{s}, s) \wedge \alpha > 0]\\
&\qquad\quad \Rightarrow [\Phi(\underline{s}, s) \wedge \exists s' \in S, k \in \mathrm{n} . t_k(s, s') \wedge (m_k > 0 \vee \mathbb{B}(m, s))])\\
&\quad \wedge\\
&\qquad ([I_{12}(\alpha, m, \underline{s}, s) \wedge \alpha > 0 \wedge t_k(s, s') \wedge ([m_k > 0 \wedge m' < k = m]\\
&\qquad\quad \vee [\mathbb{B}(m, s) \wedge m' > 0])] \Rightarrow [\exists \alpha' < \alpha . I_{12}(\alpha', m', \underline{s}, s')])\\
&\quad \wedge\\
&\qquad (I_{12}(0, m, \underline{s}, \bar{s}) \Rightarrow \Psi(\underline{s}, \bar{s}))])
\end{aligned}\right\}$$

where

$$\mathbb{B} = \lambda(m, s).[\forall j \in n.(\beta_j(s) \vee m_j = 0)]$$
$$m' <k= m \quad \text{iff} \quad (m'_k < m_k \wedge \forall j \in (\mathrm{n} \sim k).(m'_j = m_j))$$
$$m' > 0 \quad \text{iff} \quad (\forall j \in n.m'_j > 0)$$

For the standard example [[X: = **false**||**while** X **do skip od**]] where $S = \{\mathrm{tt}, \mathrm{ff}\}$, $t_1 = \lambda(x, x').[\neg x']$, $t_2 = \lambda(x, x').[x \wedge x']$, $\varepsilon = \lambda x.\mathrm{tt}$, $\Phi = \lambda(\underline{x}, x).\mathrm{tt}$, $\Psi = \lambda(\underline{x}, \bar{x}).[\neg \bar{x}]$, (12) is satisfied by $I_{12} = \lambda(\alpha, m, \underline{x}, x).[(\alpha = 0 \wedge \neg x) \vee (\alpha = m_1 + m_2 > 0)]$. □

12.4 The dynamic cutset approach for proving inevitability properties of non-closed sets of admissible complete traces

Let P be a program specified by a partitioned transition system $\langle S, \mathrm{n}, t, \varepsilon\rangle$ and a non-closed set $\theta\langle S, \mathrm{n}, t, \varepsilon\rangle \subseteq \Gamma(\Sigma\langle S, \bigvee_{k \in \mathrm{n}} t_k, \varepsilon\rangle)$ of admissible traces. If we want to prove inevitability properties of P by computational induction on t, we have to find an invariant and a termination argument.

This invariant must hold for all states that are reachable by admissible traces. Let us first consider the simple case when these states are exactly those which are reachable by successive transitions $\bigvee_{k \in \mathrm{n}} t_k$:

$$\{s \in S: \exists p \in \theta\langle S, \mathrm{n}, t, \varepsilon\rangle, i \in Dom(p).(p_i = s)\}$$
$$=$$
$$\left\{s \in S: \exists \underline{s} \in S.(\varepsilon(\underline{s}) \wedge \left(\bigvee_{k \in \mathrm{n}} t_k\right)^* (\underline{s}, s)\right\} \tag{13}$$

(where r^* is the reflexive transitive closure of relation r) which holds in particular when

$$\forall \underline{s} \in S.(\varepsilon(\underline{s}) \Rightarrow [\underline{s} \in \Gamma(\theta\langle S, \mathrm{n}, t, \varepsilon\rangle)])$$
$$\wedge$$
$$\forall m \in (\omega \sim 0), p \in (m \to S), k \in \mathrm{n}, s \in S.$$
$$([p \in \Gamma(\theta\langle S, \mathrm{n}, t, \varepsilon\rangle) \wedge t_k(p_{m-1}, s)] \Rightarrow [ps \in \Gamma(\theta\langle S, \mathrm{n}, t, \varepsilon\rangle)]) \tag{14}$$

Notice that (13) $\not\Rightarrow$ (14).

Proof. (14) ⇒ (13).

If $p \in \theta\langle S, \mathrm{n}, t, \varepsilon\rangle$ then $\varepsilon(p_0)$ and $\forall i \in Dom(p).(\bigvee_{k \in \mathrm{n}} t_k)^*(p_0, p_i)$. Reciprocally, if $\varepsilon(\underline{s}) \wedge (\bigvee_{k \in \mathrm{n}} t_k)^*(\underline{s}, s)$ then there are $m \in (\omega \sim 0)$, $p \in (m \to S)$ such that $p_0 = \underline{s}$, $\forall i \in (Dom(p) \sim 0) . \exists k \in \mathrm{n} . t_k(p_{i-1}, p_i)$ and $p_{m-1} = s$. By (14), $p_0 \in \Gamma(\theta\langle S, \mathrm{n}, t, \varepsilon\rangle)$ and if $i \in (m \sim 0)$ and $p[i] \in \Gamma(\theta\langle S, \mathrm{n}, t, \varepsilon\rangle)$ by induction hypothesis then $p[i]p_i \in \Gamma(\theta\langle S, \mathrm{n}, t, \varepsilon\rangle)$ so that $p \in \Gamma(\theta\langle S, \mathrm{n}, t, \varepsilon\rangle)$. Hence $\exists p' \in \theta\langle S, \mathrm{n}, t, \varepsilon\rangle, i \in Dom(p') . p_i = s$. □

Example

$\theta wf\langle S, \mathrm{n}, t, \varepsilon\rangle$ satisfies (14) hence (13) so that invariance proofs with fair execution hypothesis can be made without taking fairness into account. □

When (14) holds, $\bigvee_{k \in \mathrm{n}} t_k$ can be used for the invariance proof.

Let us now consider the termination argument. For finite admissible traces we have to show that the goal must be reached before the end of the trace. This is simple when admissible traces end with blocking states:

$$\forall m \in (\omega \sim 0), p \in ((\theta\langle S, \mathrm{n}, t, \varepsilon\rangle) \cap (m \to S)), k \in \mathrm{n}, s' \in S . \neg t_k(p_{m-1}, s') \tag{15}$$

or equivalently

$$\theta\langle S, \mathrm{n}, t, \varepsilon\rangle \subseteq \Sigma\langle S, \mathrm{n}, t, \varepsilon\rangle \tag{15}$$

since it is sufficient to show that blocking states cannot satisfy the invariant. For infinite admissible traces, we ensure that progress is made toward the goal by finding a termination function that decreases on a cutset of the trace. However this progress along a trace might not be continuous (e.g. when assuming fair execution) so that there may exist no such 'static' cutset (i.e. depending only upon the set S of states (e.g. loop cutsets for sequential programs)). In general, the choice of the cutpoints indicating progress toward the goal should be 'dynamic' (i.e. depends upon the trace itself so that auxiliary variables are needed to capture histories).

These remarks inspired the following induction principle:

Intuitively, for no infinite admissible trace p and auxiliary trace a on A (the first element of which is defined by F, the next ones by $\not{C}$ but for finitely many cuts defined by C) we can have the invariant I true everywhere. (The invariant I has not been incorporated into F, C and $\not{C}$ only for the sake of convenience).

Example

If $\theta\langle S, \mathrm{n}, t, \varepsilon\rangle = \Sigma\langle S, \bigvee_{k \in \mathrm{n}} t_k, \varepsilon\rangle$ and there exists $K \subseteq S$ such that $Cutset\langle S, \bigvee_{k\in \mathrm{n}} t_k, \varepsilon\rangle(K)$ then choosing $A = \{\perp\}$, $F = \lambda(\underline{s}, a).\mathrm{tt}$, $I = \lambda(s, a).\mathrm{tt}$, $C = \lambda(a, k, s, a').\mathrm{tt}$, $\not{C} = \lambda(a, l, s', a').[s' \notin K]$ and $I_3 = \lambda(\alpha, \underline{s}, s).[I_{16}(\alpha, \underline{s}, s, \perp)]$ one obtains a version of (3). □

Proof. Conditional soundness (15) ⇒ [(16) ⇒ (10)].

Assume (16) and $p \in \theta\langle S, \mathrm{n}, t, \varepsilon\rangle$. If there is $i \in Dom(p)$ such that $\Psi(p_0, p_i)$ then for the least such i there are $\alpha \in (i \to \delta)$ and $a \in (i \to A)$ such that $\forall j \in i.I_{16}(\alpha_j, p_0, p_j, a_j)$ hence $\forall j \in i.\Phi(p_0, p_j)$. It is not possible that $\forall i \in Dom(p).\neg\Psi(p_0, p_i)$. Otherwise there would be $\alpha \in (Dom(p) \to \delta)$ and $a \in (Dom(p) \to A)$ such that $F(p_0, a_0)$ and $\forall j \in Dom(p).I_{16}(\alpha_j, p_0, p_j, a_j)$ hence $\forall j \in Dom(p).I(p_j, a_j)$ and moreover $\forall j \in (Dom(p) \sim 0).\alpha_{j-1} \geq \alpha_j$. When p is finite we have $p \in \theta\langle S, \mathrm{n}, t, \varepsilon\rangle \subseteq \Gamma(\theta\langle S, \mathrm{n}, t, \varepsilon\rangle)$ and $I_{16}(\alpha_{m-1}, p_0, p_{m-1}, a_{m-1})$ where $Dom(p) = m$. This implies $\exists k \in \mathrm{n}$, $s' \in S.t_k(p_{m-1}, s')$ in contradiction with (15). When p is infinite (in which case the infinite sequence of ordinals α_j cannot be strictly decreasing) there are finitely many places $\gamma_i \in \omega$, $i \in m$, $m \in \omega$ where α_j is strictly decreased and C holds. Everywhere else $\not{C}$ would hold, in contradiction with the dynamic cutset condition (17). □

Proof. Conditional weak semantic completeness (14) ∧ (15) ⇒ [(10) ⇒ (16)].

Assume (10) and define $A = \Sigma^*\langle S\rangle$, $F = \lambda(\underline{s}, \underline{a}).[\underline{a} = \underline{s}]$, $\mathrm{I} = \lambda(s, a).[\forall i \in Dom(a).\neg\Psi(a_0, a_i)]$, $C = \not{C} = \lambda(a, k, s', a').[a' = as']$. If we can find $p \in (\theta\langle S, \mathrm{n}, t, \varepsilon\rangle \cap (\omega \to S))$, $a \in (\omega \to A)$, $m \in (\omega \sim 0)$, $\gamma \in (m \to \omega)$ not satisfying (17) then we have $F(p_0, a_0)$ hence $a_0 = p_0 = p[1]$. Assume by induction hypothesis that $a_j = p[j+1]$. Then either $(j+1) \neq \gamma_i$ for all $i \in m$ in which case

$\exists k\in \mathrm{n}.t_k(p_j, p_{j+1})\wedge \not{C}(a_j, k, p_{j+1}, a_{j+1}))$ implies $a_{j+1}=p[j+1]p_{j+1}$ whence $a_{j+1}=p[j+2]$. Else $\exists i\in m.\gamma_i=(j+1)$ so that $\gamma_i\neq 0$ hence $i\neq 0$ and $(\exists k\in \mathrm{n}.t_k(p_j, p_{j+1})\wedge C(a_j, k, p_{j+1}, a_{j+1}))$ implies $a_{j+1}=p[j+2]$. The contradiction with (10) is now that $\forall j\in\omega.I(p_j, a_j)$ whence $I(p_j, p[j+1])$ so that $\neg\Psi(p_0, p_j)$. We conclude *D-cutset* $\theta\langle S, \mathrm{n}, t, \varepsilon\rangle(A, F, I, C, \not{C})$.

Let us now choose $\delta=2$ and $I_{16}=\lambda(\alpha, \underline{s}, s, a).[(\alpha=0\wedge\Psi(\underline{s}, s))\vee(\alpha=1\wedge a\in\Gamma(\theta\langle S,\mathrm{n},t,\varepsilon\rangle)\wedge\exists m\in(\omega\sim 0).Dom(a)=m\wedge a_0=\underline{s}\wedge a_{m-1}=s\wedge[\forall i\in m.(\Phi(a_0, a_i)\wedge\neg\Psi(a_0, a_i)]])]$. Then assuming (14) and (15), I_{16} satisfies (16). □

The above completeness result is weak in the sense that the cutset that is chosen for the completeness proof depends upon the property Ψ which is proved to be inevitable.

It is sometimes possible to find auxiliary variables and a corresponding dynamic cutset which is adequate for proving any inevitable property for a given class of admissible traces.

Example

If $\theta\langle S, \mathrm{n}, t, \varepsilon\rangle=\theta wf\langle S, \mathrm{n}, t, \varepsilon\rangle$ then one can choose $A=n$, $F=\lambda(s, l).\mathrm{tt}$ $I=\lambda(s, l).[\exists s'\in S.t_l(s, s')]$, $C=\lambda(l, k, s', l').\mathrm{tt}$ and $\not{C}=\lambda(l, k, s', l').[l\neq k\wedge l'=l]$.

If there are $p\in\theta wf\langle S, \mathrm{n}, t, \varepsilon\rangle$ and $l\in(Dom(p)\to\mathrm{n})$ not satisfying the cutset condition (17) then either $Dom(p)=j\in(\omega\sim 0)$ so that p_{j-1} is a blocking state in contradiction with $I(p_{j-1}, l_{j-1})$ or $Dom(p)=\omega$ in which case there is some $k=l_{\gamma_{m-1}}$ such that t_k is continuously enabled $(\forall j\geq\gamma_{m-1}, l_j=k$ so that $I(p_j, l_j)$ implies $\exists s'\in S.t_k(p_j, s'))$ and never activated $(\forall j>\gamma_{m-1}, \exists i\in\mathrm{n}.t_i(p_{j-1}, p_j)\wedge\not{C}(l_{j-1}, i, p_j, l_j)$ so that $i\neq k)$, in contradiction with the weak fairness hypothesis.

Replacing A, F, I, C, $\not{C}$ in (16) by the above definitions we get:

$$\left.\begin{array}{l}
(\exists\delta\in Ord, I_{18}\in(\delta\times S\times S\times\mathrm{n}\to\{\mathrm{tt},\mathrm{ff}\}).\\
\quad(\forall\underline{s}, s\in S, \alpha<\delta, l\in\mathrm{n}.\\
\qquad(\varepsilon(\underline{s})\Rightarrow[\exists\underline{\alpha}<\delta, \underline{l}\in\mathrm{n}.I_{18}(\underline{\alpha}, \underline{s}, \underline{s}, \underline{l})])\\
\quad\wedge\\
\qquad(I_{18}(\alpha, \underline{s}, s, l)\Rightarrow\quad\Psi(\underline{s}, s)\\
\qquad\qquad\qquad\qquad\qquad\vee\\
\qquad\qquad\qquad\qquad\qquad[\Phi(\underline{s}, s)\wedge\exists s'\in S.\,t_l(s, s')\\
\qquad\qquad\qquad\qquad\qquad\quad\wedge\forall k\in\mathrm{n}, s'\in S.(t_k(s, s')\Rightarrow\\
\qquad\qquad\qquad\qquad\qquad\qquad[(\exists\alpha'<\alpha, l'\in\mathrm{n}.I_{18}(\alpha', \underline{s}, s', l'))\vee\\
\qquad\qquad\qquad\qquad\qquad\qquad(l\neq k\wedge I_{18}(\alpha, \underline{s}, s', l))])])))
\end{array}\right\}\quad(18)$$

$\exists k \in \mathrm{n}\,.\,t_k(p_j, p_{j+1}) \wedge \not{C}(a_j, k, p_{j+1}, a_{j+1}))$ implies $a_{j+1} = p[j+1]\,p_{j+1}$ whence $a_{j+1} = p[j+2]$. Else $\exists i \in m\,.\,\gamma_i = (j+1)$ so that $\gamma_i \neq 0$ hence $i \neq 0$ and $(\exists k \in \mathrm{n}\,.\,t_k(p_j, p_{j+1}) \wedge C(a_j, k, p_{j+1}, a_{j+1}))$ implies $a_{j+1} = p[j+2]$. The contradiction with (10) is now that $\forall j \in \omega\,.\,I(p_j, a_j)$ whence $I(p_j, p[j+1])$ so that $\neg\Psi(p_0, p_j)$. We conclude *D-cutset* $\theta\langle S, \mathrm{n}, t, \varepsilon\rangle(A, F, I, C, \not{C})$.

Let us now choose $\delta = 2$ and $I_{16} = \lambda(\alpha, \underline{s}, s, a)\,.\,[(\alpha = 0 \wedge \Psi(\underline{s}, s)) \vee (\alpha = 1 \wedge a \in \Gamma(\theta\langle S,\mathrm{n},t,\varepsilon\rangle) \wedge \exists m \in (\omega \sim 0)\,.\,Dom(a) = m \wedge a_0 = \underline{s} \wedge a_{m-1} = s \wedge [\forall i \in m\,.\,(\Phi(a_0, a_i) \wedge \neg\Psi(a_0, a_i)]])]$. Then assuming (14) and (15), I_{16} satisfies (16). □

The above completeness result is weak in the sense that the cutset that is chosen for the completeness proof depends upon the property Ψ which is proved to be inevitable.

It is sometimes possible to find auxiliary variables and a corresponding dynamic cutset which is adequate for proving any inevitable property for a given class of admissible traces.

Example

If $\theta\langle S, \mathrm{n}, t, \varepsilon\rangle = \theta wf\langle S, \mathrm{n}, t, \varepsilon\rangle$ then one can choose $A = n$, $F = \lambda(s, l)\,.\,\mathrm{tt}$ $I = \lambda(s, l)\,.\,[\exists s' \in S\,.\,t_l(s, s')]$, $C = \lambda(l, k, s', l')\,.\,\mathrm{tt}$ and $\not{C} = \lambda(l, k, s', l')\,.\,[l \neq k \wedge l' = l]$.

If there are $p \in \theta wf\langle S, \mathrm{n}, t, \varepsilon\rangle$ and $l \in (Dom(p) \rightarrow \mathrm{n})$ not satisfying the cutset condition (17) then either $Dom(p) = j \in (\omega \sim 0)$ so that p_{j-1} is a blocking state in contradiction with $I(p_{j-1}, l_{j-1})$ or $Dom(p) = \omega$ in which case there is some $k = l_{\gamma_{m-1}}$ such that t_k is continuously enabled $(\forall j \geq \gamma_{m-1}, l_j = k$ so that $I(p_j, l_j)$ implies $\exists s' \in S\,.\,t_k(p_j, s'))$ and never activated $(\forall j > \gamma_{m-1}, \exists i \in \mathrm{n}\,.\,t_i(p_{j-1}, p_j) \wedge \not{C}(l_{j-1}, i, p_j, l_j)$ so that $i \neq k)$, in contradiction with the weak fairness hypothesis.

Replacing A, F, I, C, $\not{C}$ in (16) by the above definitions we get:

$$\left.\begin{array}{l}
(\exists \delta \in Ord, I_{18} \in (\delta \times S \times S \times \mathrm{n} \rightarrow \{\mathrm{tt}, \mathrm{ff}\}). \\
\quad (\forall \underline{s}, s \in S, \alpha < \delta, l \in \mathrm{n}. \\
\qquad (\varepsilon(\underline{s}) \Rightarrow [\exists \underline{\alpha} < \delta, \underline{l} \in \mathrm{n}\,.\,I_{18}(\underline{\alpha}, \underline{s}, \underline{s}, \underline{l})]) \\
\quad\; \wedge \\
\qquad (I_{18}(\alpha, \underline{s}, s, l) \Rightarrow \quad \Psi(\underline{s}, s) \\
\qquad\qquad\qquad\qquad\quad \vee \\
\qquad\qquad\qquad\qquad\quad [\Phi(\underline{s}, s) \wedge \exists s' \in S\,.\,t_l(s, s') \\
\qquad\qquad\qquad\qquad\qquad \wedge \forall k \in \mathrm{n}, s' \in S\,.\,(t_k(s, s') \Rightarrow \\
\qquad\qquad\qquad\qquad\qquad\quad [(\exists \alpha' < \alpha, l' \in \mathrm{n}\,.\,I_{18}(\alpha', \underline{s}, s', l')) \vee \\
\qquad\qquad\qquad\qquad\qquad\quad (l \neq k \wedge I_{18}(\alpha, \underline{s}, s', l))])])))
\end{array}\right\} (18)$$

A version of (18) was proposed by Lehmann, Pnueli & Stavi [9] and their semantic completeness proof is easy to adapt. This proof is independent of Φ and Ψ. □

Let us now consider the general case.

For soundness, verification conditions (16) have to be strengthened when (15) does not hold. It must be ensured that for finite admissible traces the goal must be reached before the end of the trace (which may not be a blocking state).

For completeness, verification conditions (16) have to be weakened when (14) does not hold. The invariant must hold for all states that are reachable by an admissible trace but may not hold for states that are reachable by successive transitions $\bigvee_{k \in \mathrm{n}} t_k$:

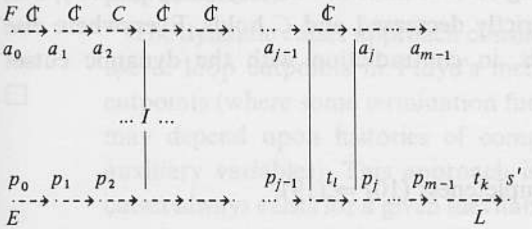
$$
\left.
\begin{array}{l}
(\exists E \in (S \to \{\mathrm{tt}, \mathrm{ff}\}),\ A,\ F \in (S \times A \to \{\mathrm{tt}, \mathrm{ff}\}),\\
I \in (S \times A \to \{\mathrm{tt}, \mathrm{ff}\}),\ L, R \in (S \times A \times \mathrm{n} \times S \to \{\mathrm{tt}, \mathrm{ff}\}),\\
C, \not{C} \in (A \times \mathrm{n} \times S \times A \to \{\mathrm{tt}, \mathrm{ff}\}).\\
\qquad \mathit{Entry} \quad \theta\langle S, \mathrm{n}, t, \varepsilon\rangle(E)\\
\quad \wedge\\
\qquad \mathit{Live} \quad \theta\langle S, \mathrm{n}, t, \varepsilon\rangle(A, F, I, C, \not{C})(L)\\
\quad \wedge\\
\qquad \mathit{Next} \quad \theta\langle S, \mathrm{n}, t, \varepsilon\rangle(A, F, I, C, \not{C})(R)\\
\quad \wedge\\
\qquad \mathit{D\text{-}cutset} \quad \theta\langle S, \mathrm{n}, t, \varepsilon\rangle(A, F, I, C, \not{C})\\
\quad \wedge\\
\qquad (\exists \delta \in \mathit{Ord},\ I_{19} \in (\delta \times S \times S \times A \to \{\mathrm{tt}, \mathrm{ff}\}).\\
\qquad\qquad (\forall \underline{s}, s \in S, \alpha < \delta, a \in A.\\
\qquad\qquad\qquad (E(\underline{s}) \Rightarrow [\exists \underline{\alpha} < \delta, \underline{a} \in A.(F(\underline{s}, \underline{a}) \wedge I_{19}(\underline{\alpha}, \underline{s}, \underline{s}, \underline{a}))]\\
\qquad\qquad \wedge\\
\qquad\qquad\qquad (I_{19}(\alpha, \underline{s}, s, a) \Rightarrow \quad \Psi(\underline{s}, s)\\
\qquad\qquad\qquad\qquad\qquad\qquad \vee\\
\qquad\qquad\qquad\qquad\qquad\qquad [\Phi(\underline{s}, s) \wedge I(s, a)\\
\qquad\qquad\qquad\qquad\qquad\qquad \wedge\\
\qquad\qquad\qquad\qquad\qquad\qquad \exists k \in \mathrm{n}, s' \in S.[t_k(s, s')\\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \wedge\ L(s, a, k, s')]\\
\qquad\qquad\qquad\qquad\qquad\qquad \wedge\\
\qquad\qquad\qquad\qquad\qquad\qquad \forall k \in \mathrm{n}, s' \in S.([t_k(s, s')\\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \wedge\ R(s, a, k, s')] \Rightarrow\\
\qquad\qquad\qquad\qquad\qquad\qquad [(\exists \alpha' < \alpha, a' \in A.C(a, k, s', a')\\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \wedge\ I_{19}(\alpha', \underline{s}, s', a'))\\
\qquad\qquad\qquad\qquad\qquad\qquad \vee\\
\qquad\qquad\qquad\qquad\qquad\qquad (\exists a' \in A.\not{C}(a, k, s', a')\\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \wedge\ I_{19}(\alpha, \underline{s}, s', a'))])]))))
\end{array}
\right\} \quad (19)
$$

where

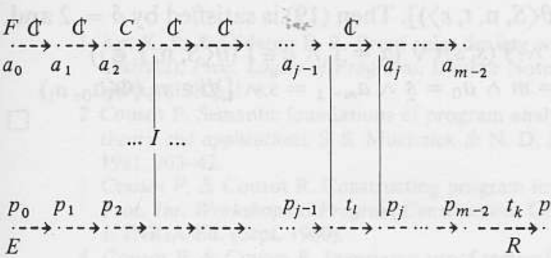
$$\textit{Entry}\quad \theta\langle S, \mathrm{n}, t, \varepsilon\rangle(E) = [\forall p \in \theta\langle S, \mathrm{n}, t, \varepsilon\rangle . E(p_0)] \tag{20}$$

$$\begin{aligned}&\textit{Live}\quad \theta\langle S, \mathrm{n}, t, \varepsilon\rangle(A, F, I, C, \not{C})(L) = \\ &\quad (\forall m \in (\omega \sim 0),\ p \in (\Gamma(\theta\langle S, \mathrm{n}, t, \varepsilon\rangle) \cap (m \to S)),\ a \in (m \to A),\ k \in \mathrm{n}, \\ &\hspace{28em} s' \in S. \\ &\quad [F(p_0, a_0) \wedge \forall j \in m . I(p_j, a_j) \wedge \forall j \in (m \sim 0) . [\exists l \in \mathrm{n}.\ t_l(p_{j-1}, p_j) \wedge \\ &\qquad (\not{C}(a_{j-1}, l, p_j, a_j) \vee C(a_{j-1}, l, p_j, a_j)) \wedge t_k(p_{m-1}, s') \wedge \\ &\qquad L(p_{m-1}, a_{m-1}, k, s')] \Rightarrow [p \notin \theta\langle S, \mathrm{n}, t, \varepsilon\rangle]) \end{aligned} \tag{21}$$

A formula better understood with the help of the following schema:



$$\begin{aligned}&\textit{Next}\quad \theta\langle S, \mathrm{n}, t, \varepsilon\rangle(A, F, I, C, \not{C})(R) = \\ &\quad (\forall p \in \Gamma(\theta\langle S, \mathrm{n}, t, \varepsilon\rangle),\ m \in \omega . (\mathit{Dom}(p) = m \wedge m > 1) \Rightarrow \\ &\qquad (\forall a \in ((m-1) \to A),\ k \in \mathrm{n}. \\ &\qquad [F(p_0, a_0) \wedge \forall j \in (m-1) . I(p_j, a_j) \wedge \forall j \in ((m-1) \sim 0) . [\exists l \in \mathrm{n}. \\ &\qquad t_l(p_{j-1}, p_j) \\ &\qquad \wedge (\not{C}(a_{j-1}, l, p_j, a_j) \vee C(a_{j-1}, l, p_j, a_j))] \\ &\qquad \wedge t_k(p_{m-2}, p_{m-1})] \\ &\qquad \Rightarrow R(p_{m-2}, a_{m-2}, k, p_{m-1}))) \end{aligned} \tag{22}$$



Proof. Soundness (19) ⇒ (10).

Assume (19), $p \in \theta\langle S, \mathrm{n}, t, \varepsilon\rangle$ and $\forall i \in \mathit{Dom}(p) . \neg\Psi(p_0, p_i)$. Let $\mathrm{Inv}(d)$ be $[\exists \alpha \in (d \to \delta), a \in (d \to A) . F(p_0, a_0) \wedge \forall j \in d . I(p_j, a_j) \wedge \forall j \in (d \sim 0) . (\exists l \in n.$ $t_l(p_{j-1}, p_j) \wedge (\not{C}(a_{j-1}, l, p_j, a_j) \vee C(a_{j-1}, l, p_j, a_j))) \wedge \forall j \in d . I_{19}(\alpha_j, p_0,$ $p_j, a_j) \wedge \forall j \in (d \sim 0) . \alpha_j \leq \alpha_{j-1}]$. We have $\mathrm{Inv}(\mathit{Dom}(p))$. This is because $E(p_0)$ holds by (20) hence $\mathrm{F}(p_0, a_0) \wedge I_{19}(\alpha_0, p_0, p_0, a_0)$ is true by (19). Assume $\mathrm{Inv}(m-1)$ by induction hypothesis and $m \in \mathit{Dom}(p)$. We have

$t_k(p_{m-1}, p_m)$ for some $k \in n$, hence by (22), $R(p_{m-1}, a_{m-1}, k, p_m)$ hence by (19) either there are $\alpha_m < \alpha_{m-1}$, $a_m \in A$ such that $C(a_{m-1}, k, p_m, a_m)$ or $\alpha_m = \alpha_{m-1}$ and there is $a_m \in A$ such that $\not C(a_{m-1}, k, p_m, a_m)$ and in both cases $I_{19}(\alpha_m, p_0, p_m, a_m)$. Again (19) and $\neg \Psi(p_0, p_m)$ imply $I(p_m, a_m)$ hence $\mathrm{Inv}(m)$.

If $Dom(p) \in \omega$ then $\mathrm{Inv}(m)$ and (19) imply $\exists k \in \mathrm{n}$, $s' \in \mathrm{n}$. $[t_k(p_{m-1}, s') \wedge L(p_{m-1}, a_{m-1}, k, s')$ which according to (21) is in contradiction with $p \in \theta\langle S, \mathrm{n}, t, \varepsilon\rangle$.

If $Dom(p) = \omega$ then $\mathrm{Inv}(\omega)$ and the infinite sequence of ordinals α_j cannot be strictly decreasing so that there are finitely many places $\gamma_i \in \omega$, $i \in m$, $m \in \omega$ where α_j is strictly decreased and C holds. Everywhere else (19) implies that $\not C$ holds, in contradiction with the dynamic cutset condition (17). □

Proof. Weak semantic completeness (10) ⇒ (19).

Assume (10) and define $A = \Sigma^*\langle S\rangle$, $F = \lambda(\underline{s}, \underline{a}).[\underline{a} = \underline{s}\}$, $I = \lambda(s, a).[\forall i \in Dom(p).\neg \Psi(a_0, a_i)]$ and $C = \not C = \lambda(a, k, s', a').[a' = as']$. We observe that $\forall d \in ((\omega + 1) \sim 0)$, $p \in (\Gamma(\theta\langle S, \mathrm{n}, t, \varepsilon\rangle) \cap (d \to S))$, $a \in (d \to A).([F(p_0, a_0) \wedge \forall j \in d.I(p_j, \underline{a}_j) \wedge \forall j \in (d \sim 0).[\exists l \in \mathrm{n}.t_l(p_{j-1}, p_j) \wedge (\not C(a_{j-1}, l, p_j, a_j) \vee C(a_{j-1}, l, p_j, a_j))]] \Rightarrow (p = a))$. It follows that *D-cutset* $\theta\langle S, \mathrm{n}, t, \varepsilon\rangle(A, F, I, C, \not C)$ because Ψ is inevitable by (10). The same way (20) follows from the choice $E = \lambda\underline{s}.[\underline{s} \in \Gamma(\theta\langle S, \mathrm{n}, t, \varepsilon\rangle)]$, (21) follows from $L = \lambda(s, a, k, s').[a \notin \theta\langle S, \mathrm{n}, t, \varepsilon\rangle]$ and (22) from $R = \lambda(s, a, k, s').[as' \in \Gamma(\theta\langle S, \mathrm{n}, t, \varepsilon\rangle)]$. Then (19) is satisfied by $\delta = 2$ and $I_{19} = \lambda(\alpha, \underline{s}, s, a).[(\alpha = 0 \wedge \Psi(\underline{s}, s)) \vee (\alpha = 1 \wedge a \in \Gamma(\theta\langle S, \mathrm{n}, t, \in\rangle)$ $\wedge \exists m \in (\omega \sim 0).Dom(a) = m \wedge a_0 = \underline{s} \wedge a_{m-1} = s \wedge [\forall i \in m.(\Phi(a_0, a_i)$ $\wedge \neg \Psi(a_0, a_i)]])]$. □

13 Conclusion

We have considered the problem of proving inevitability properties of programs, the behavior of which is specified by a set of sequences of states.

When this set of traces is closed, it can be generated by a transition relation on the program states so that inevitability properties can be proved using any one of the numerous equivalent, sound and complete variants of Floyd's basic 'invariant assertions and well-ordered set' method.

When this set of traces is not closed (e.g. fair parallelism) we have considered two sound approaches:

The transformational approach consists in using Floyd's method for a transition relation on program states and auxiliary variables that exactly generates this set of traces. Although the derived method is complete, it may have the severe practical defect that the auxiliary transition relation may not be computable (so that e.g. this auxiliary transition relation may not be representable by a program derived from the original one which is proved correct).

The dynamic cutset approach consists in a generalization of the use of loop cutpoints in Floyd's method, in that the choice of cutpoints (where some termination function has to be decreased) may depend upon histories of computations (cumulated into auxiliary variables). This approach is weakly complete since a cutset always exists for a given inevitability property but no cutset may be valid for all of them. The problem of characterizing the classes of program behaviors for which a dynamic cutset can be found that is valid for all inevitability properties is interesting and left open.

References

1 Apt K. R. & Olderog E. R. Proof rules dealing with fairness (extended abstract), *Proc. Logics of Programs*, Lecture Notes in Comp. Sci. 131, Springer-Verlag (1982), 1–8.

2 Cousot P. Semantic foundations of program analysis. In *Program flow analysis, theory and applications*, S. S. Muchnick & N. D. Jones (Eds), Prentice-Hall, 1981, 303–42.

3 Cousot P. & Cousot R. Constructing program invariance proof methods. *Proc. Int. Workshop on Program Construction*, Château de Bonas, France, vol. 1, INRIA Ed. (Sept. 1980).

4 Cousot P. & Cousot R. Invariance proof methods and analysis techniques for parallel programs, in *Automatic program construction techniques*, A. W. Bierman, G. Guiho & Y. Kodratoff (Eds), Macmillan (1984), 243–72.

5 Dijkstra E. W. *A discipline of programming*, Prentice-Hall, 1976.

6 Floyd R. W. Assigning meanings to programs. *Proc. AMS Symp. in Applied Mathematics*, **19** (1967), 19–32.

7 Lamport L. Proving the correctness of multiprocess programs. *IEEE Trans. on Soft Eng.* **3**(2) (1977), 125–43.

8 Lamport L. The Hoare logic of concurrent programs. *Acta Informatica*, **14** (1980), 21–37.

9 Lehmann D., Pnueli A. & Stavi J. Impartiality, justice and fairness: the ethics of concurrent termination. *Proc. 8th Coll. on Automata, Languages and Programming*, Lect. Notes in Comp. Sci. 115, Springer-Verlag (1981), 264-77.

10 Naur P. Proof of algorithms by general snapshots. *BIT*, **6** (1966), 310–16.

11 Owicki S. & Gries D. An axiomatic proof technique for parallel programs I. *Acta Informatica*, **6** (1976), 319–40.

12 Park D. A predicate transformer for weak fair iteration. *Proc. 6th IBM Symp. on Math. Foundations of Comp. Sci., Logical aspects of programs*, Hakone, Japan (May 1981), 259–75.

13 Plotkin G. D. A power domain for countable non-determinism (extended abstract). *ICALP 81*, Lecture Notes in Comp. Sci., Springer-Verlag (1981).