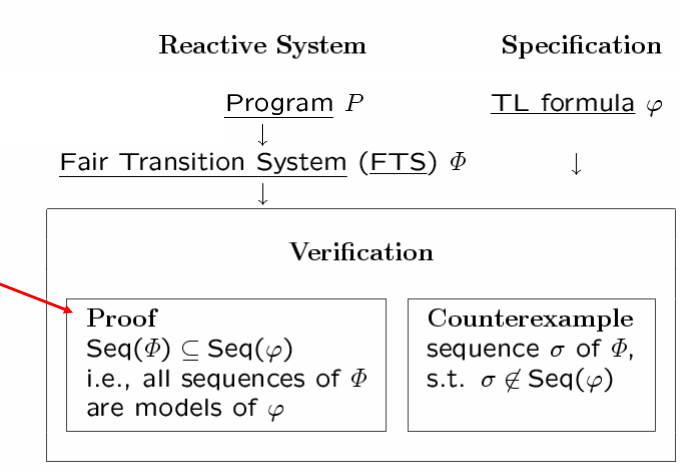
Verification – Lecture 4
Proving Invariance Properties II

Bernd Finkbeiner – Sven Schewe
Rayna Dimitrova – Lars Kuhtz – Anne Proetzsch

Wintersemester 2007/2008

Big Picture



Proof rules reduce P-validity of specification to

State-validity of verification conditions

Proving Invariance

Review

For assertion q,

B1. $P \models \Theta \rightarrow q$

B2. $P \models \{q\}\ \mathcal{T}\ \{q\}$

$P \models \Box q$ B-INV

- for $\tau \in \mathcal{T}$ in P
  $\{\varphi\}\tau\{\psi\}$: $\rho_\tau \wedge \varphi \rightarrow \psi'$
  "τ leads from φ to ψ in P"
- for $\mathcal{T}$ in P
  $\{\varphi\}\mathcal{T}\{\psi\}$: $\{\varphi\}\tau\{\psi\}$ for every $\tau \in \mathcal{T}$
  "$\mathcal{T}$ leads from φ to ψ in P"

Review: Runs

Review

Infinite sequence of states

σ: $s_0, s_1, s_2, \ldots$

is a run of a transition system, if it satisfies the following:

- Initiality: s_0 satisfies θ
- Consecution: For each i= 0,1, …

there is a transition $\tau \in \mathcal{T}$ s.t. $s_{i+1} \in \tau(s_i)$

Example: REQUEST-RELEASE

Review

$$\textbf{local}\ \ x\text{: integer where } x = 1$$

$$\begin{bmatrix} \ell_0: & \textbf{request } x \\ \ell_1: & \textbf{critical} \\ \ell_2: & \textbf{release } x \\ \ell_3: & \end{bmatrix}$$

$P \models \Box \underbrace{x \geq 0}_{q}$

Θ: $x = 1 \ \wedge \ \pi = \{\ell_0\}$

$\mathcal{T}$: $\{\tau_I, \tau_{\ell_0}, \tau_{\ell_1}, \tau_{\ell_2}\}$

Example: REQUEST-RELEASE

Review

B1: $\underbrace{x = 1 \wedge \pi = \{\ell_0\}}_{\Theta} \ \rightarrow \ \underbrace{x \geq 0}_{q}$

B2:

τ_I: $\underbrace{x \geq 0}_{q} \ \wedge \ \underbrace{x' = x \wedge \pi' = \pi}_{\rho_{\tau_I}} \ \rightarrow \ \underbrace{x' \geq 0}_{q'}$

τ_{ℓ_0}: $\underbrace{x \geq 0}_{q} \ \wedge \ \underbrace{move(\ell_0, \ell_1) \wedge x > 0 \wedge x' = x - 1}_{\rho_{\tau_{\ell_0}}} \ \rightarrow \ \underbrace{x' \geq 0}_{q'}$

τ_{ℓ_1}: $\underbrace{x \geq 0}_{q} \ \wedge \ \underbrace{move(\ell_1, \ell_2) \wedge x' = x}_{\rho_{\tau_{\ell_1}}} \ \rightarrow \ \underbrace{x' \geq 0}_{q'}$

τ_{ℓ_2}: $\underbrace{x \geq 0}_{q} \ \wedge \ \underbrace{move(\ell_2, \ell_3) \wedge x' = x + 1}_{\rho_{\tau_{\ell_2}}} \ \rightarrow \ \underbrace{x' \geq 0}_{q'}$

Example: REQUEST-RELEASE

Review

$$\textbf{local}\ \ x\text{: integer where } x = 1$$

$$\left[\begin{array}{ll} \ell_0: & \textbf{request } x \\ \ell_1: & \textbf{critical} \\ \ell_2: & \textbf{release } x \\ \ell_3: & \end{array}\right]$$

$P \models \Box \underbrace{x \geq 0}_{q}$ √

Let's try

$P \models \Box \underbrace{(at\_\ell_1 \rightarrow\ x = 0)}_{q}$

Attempt #1

Review

B1: $\underbrace{x = 1 \wedge \pi = \{\ell_0\}}_{\Theta} \rightarrow \underbrace{at\_\ell_1 \rightarrow x = 0}_{q}$

holds since $\pi = \{\ell_0\} \rightarrow at\_\ell_1 = \text{F}$

B2: $\{q\}\tau_{\ell_0}\{q\}$

$$\underbrace{at\_\ell_1 \rightarrow x = 0}_{q} \wedge \underbrace{move(\ell_0, \ell_1) \wedge x > 0 \wedge x' = x - 1}_{\rho_{\tau_{\ell_0}}}$$

$$\rightarrow \underbrace{at'\_\ell_1 \rightarrow x' = 0}_{q'}$$

we have $move(\ell_0, \ell_1) \rightarrow at'\_\ell_1 = \text{T}$

BUT

$(at\_\ell_1 \rightarrow x = 0) \wedge x > 0 \wedge x' = x - 1 \rightarrow x' = 0$

Cannot prove: not state-valid

Inductive Assertions

Review

For assertion q,

$$\text{B1.} \quad P \models \Theta \rightarrow q$$

$$\text{B2.} \quad P \models \{q\}\ \mathcal{T}\ \{q\}$$

$$\frac{}{P \vdash \Box q} \quad \text{B-INV}$$

- q is inductive if B1 and B2 are (state) valid
- By rule B-INV,
  every inductive assertion q is P-invariant
- The converse is not true

Example: REQUEST-RELEASE

Review

$$P \vdash \Box \underbrace{(at\_\ell_1 \rightarrow x = 0)}_{q}$$

q is not inductive.

B2: $\{q\}\tau_{\ell_0}\{q\}$

$$\underbrace{at\_\ell_1 \rightarrow x = 0}_{q} \wedge \underbrace{move(\ell_0, \ell_1) \wedge x > 0 \wedge x' = x - 1}_{\rho_{\tau_{\ell_0}}}$$

$$\rightarrow \underbrace{at'\_\ell_1 \rightarrow x' = 0}_{q'}$$

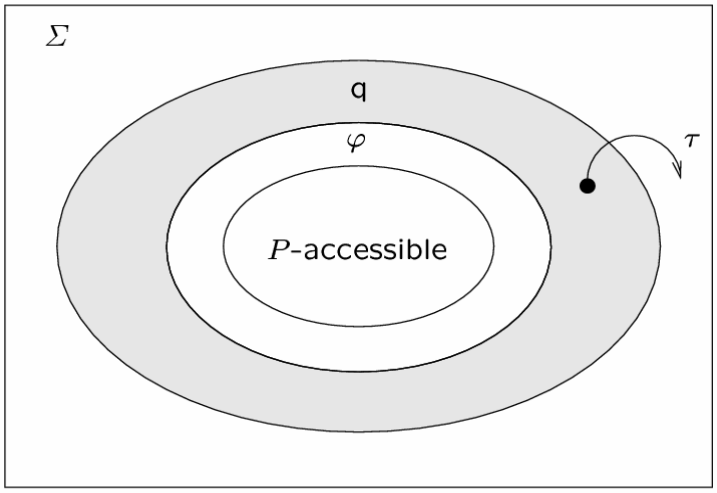
is not state valid, but it is P-state valid.

Two strategies:

1. Strengthening
2. Incremental Proofs

Strategy 1: Strengthening

Review



Find a stronger assertion φ that is inductive and implies the assertion q we want to prove.

Rules

Review

For assertions q_1, q_2,

$$\frac{P \models \Box q_1 \qquad P \Vdash q_1 \rightarrow q_2}{P \models \Box q_2}$$

MON-I

For assertions q, φ

$$\frac{\begin{array}{ll} \text{I1.} & P \Vdash \varphi \rightarrow q \\ \text{I2.} & P \Vdash \Theta \rightarrow \varphi \\ \text{I3.} & P \Vdash \{\varphi\}\ \mathcal{T}\ \{\varphi\} \end{array}}{P \models \Box q}$$

INV

Example: REQUEST-RELEASE

Review

local x: **integer** **where** $x = 1$

$$\begin{bmatrix} \ell_0: & \textbf{request } x \\ \ell_1: & \textbf{critical} \\ \ell_2: & \textbf{release } x \\ \ell_3: & \end{bmatrix}$$

$$P \models \Box \underbrace{(at\_\ell_1 \rightarrow x = 0)}_{q}$$

inductive assertion that implies

$$q: \; at\_\ell_1 \rightarrow x = 0$$

is

$$\varphi: \; (at\_\ell_1 \rightarrow x = 0) \wedge (at\_\ell_0 \rightarrow x = 1)$$

Example (cont'd)

Review

Consider $\{\varphi\}\ \tau_{\ell_0}\ \{\varphi\}$:

$$\underbrace{(at\_\ell_0 \rightarrow x = 1) \wedge (at\_\ell_1 \rightarrow x = 0)}_{\varphi} \wedge$$

$$\underbrace{move(\ell_0, \ell_1) \wedge x > 0 \wedge x' = x - 1}_{\rho_{\tau_{\ell_0}}}$$

$$\rightarrow \underbrace{(at'\_\ell_0 \rightarrow x' = 1) \wedge (at'\_\ell_1 \rightarrow x' = 0)}_{\varphi'}$$

$move(\ell_0, \ell_1)$ implies $\ell_0 \in \pi, \ell_0 \notin \pi', \ell_1 \in \pi'$

Therefore

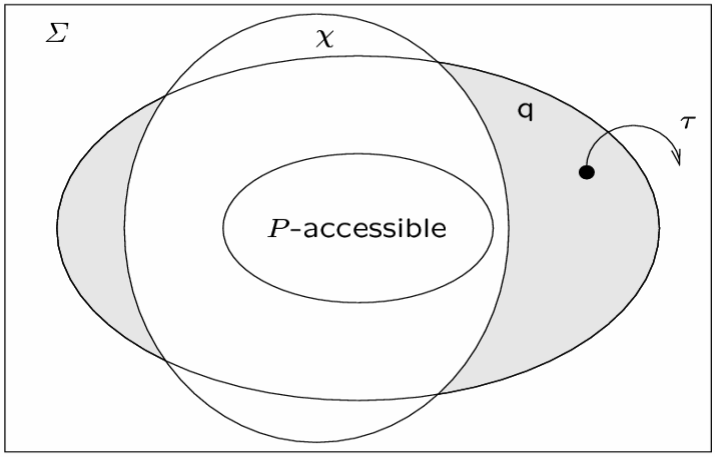
$(\mathrm{T} \rightarrow x = 1) \wedge \ldots \wedge x' = x - 1 \wedge x > 0$

$\rightarrow (\mathrm{F} \rightarrow \ldots) \wedge (\mathrm{T} \rightarrow x' = 0)$

holds.

Strategy 2: Incremental Proofs

Review



Use previously proven invariances χ to exclude parts of the state space from consideration.

Rules

Review

For assertions q_1, q_2 and χ,

$$\frac{P \models \Box\chi \qquad \models \chi \wedge q_1 \rightarrow q_2}{P \models \Box(q_1 \rightarrow q_2)}$$

SV-PSV

For assertions q_1 and q_2,

$$\frac{P \models \Box q_1 \qquad P \models \Box q_2}{P \models \Box(q_1 \wedge q_2)}$$

I-CON

Combining the Strategies

Review

For assertions $q, \varphi, \chi_1, \ldots, \chi_k$

I0. $P \models \Box\chi_1, \ldots, \Box\chi_k$

I1. $P \Vdash (\bigwedge_{i=1}^{k} \chi_i) \wedge \varphi \rightarrow q$

I2. $P \Vdash \Theta \rightarrow \varphi$

I3. $P \Vdash \{(\bigwedge_{i=1}^{k} \chi_i) \wedge \varphi\}\ \mathcal{T}\ \{\varphi\}$

$P \models \Box q$

INC-INV

Finding Inductive Invariants

Review

Construction of inductive assertions by

1. Bottom-up methods:
   - Based on program text only
   - Algorithmic
   - Guaranteed to produce an inductive invariant
2. Top-down methods:
   - Guided by the property we want to prove
   - Heuristic
   - Not guaranteed to produce an inductive invariant

Top-Down Approach

Review

previously proven $\Box\chi$

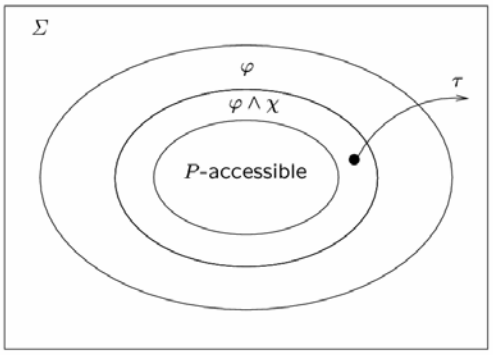
want to prove $\Box\varphi$

but

$$\{\chi \wedge \varphi\}\tau\{\varphi\}$$

not state-valid

for some $\tau \in \mathcal{T}$.

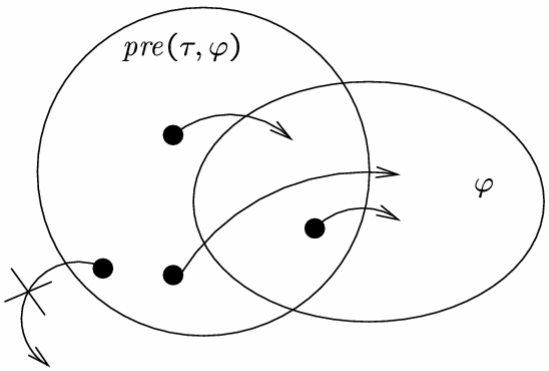


Solution: Take the largest set of states that will result in a φ-state when τ is taken.

Precondition

Review

$pre(\tau, \varphi)$: $\forall V' . \rho_\tau \rightarrow \varphi'$



a state s satisfies $pre(\tau, \varphi)$
iff
all τ-successors of s satisfy φ.

Example

Review

$V : \{x\}$

$\rho_\tau : x > 0 \ \wedge \ x' = x - 1$

$\varphi : x \geq 2$

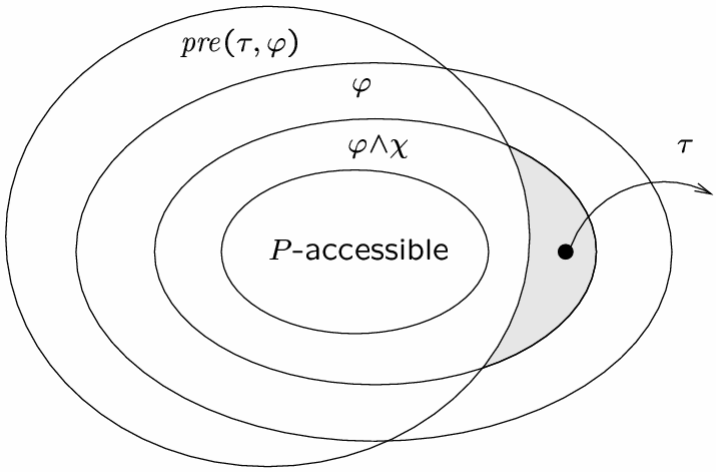
$pre(\tau, \varphi)$:

$$\forall x' . \ \underbrace{x > 0 \ \wedge \ x' = x - 1}_{\rho_\tau} \ \rightarrow \ \underbrace{x' \geq 2}_{\varphi'}$$

$$x > 0 \ \rightarrow \ x - 1 \geq 2$$

$$x \leq 0 \ \vee \ x \geq 3$$

Properties of Precondition



$\{\chi \wedge \varphi \wedge pre(\tau, \varphi)\} \ \tau \ \{\varphi\}$
is guaranteed to be state-valid.

Properties of Precondition

Claim: If φ is P-invariant then so is $pre(\tau, \varphi)$ for every $\tau \in \mathcal{T}$.

Proof:
Suppose φ is P-invariant, but $pre(\tau, \varphi)$ is not P-invariant.

Then there exists a P-accessible state s such that $s \not\models pre(\tau, \varphi)$.

But then, by the definition of $pre(\tau, \varphi)$, there exists a τ-successor s' of s such that $s' \not\models \varphi$.

Since s is P-accessible, s' is also P-accessible, contradicting that φ is a P-invariant.

Properties of Precondition

Definition: A transition τ is said to be self-disabling if for every state s, τ is disabled in all τ-successors of s.

Claim: For every assertion φ and self-disabling transition τ

$$\{\varphi \wedge pre(\tau, \varphi)\}\ \tau\ \{\varphi \wedge pre(\tau, \varphi)\}$$

is state-valid.

Proof

Assume $s \models \varphi \wedge pre(\tau, \varphi)$.

Then by definition of $pre(\tau, \varphi)$,
$s' \models \varphi$.

Since τ is self-disabling, τ is disabled in all τ-successors s' of s, and so trivially
$s' \models pre(\tau, \varphi)$

Thus for all τ-successors s' of s,
$s' \models \varphi \wedge pre(\tau, \varphi)$.

Heuristic

If the verification condition

$$\{\chi \wedge \varphi\}\tau\{\varphi\}$$

is not state-valid

- Strengthening approach:
  strengthen φ by adding the conjunct $pre(\tau, \varphi)$
- Incremental approach:
  prove $\Box\, pre(\tau, \varphi)$ and add $pre(\tau, \varphi)$ to χ.

Example

$$\textbf{local } x\text{: } \textbf{integer where } x = 1 \quad \left[\begin{array}{l} \ell_0 : \textbf{request } x \\ \ell_1 : \textbf{critical} \\ \ell_2 : \textbf{release } x \end{array}\right]$$

$$\square \underbrace{(at\_\ell_1 \rightarrow x = 0)}_{\varphi}$$

Problem:

$\{at\_\ell_1 \rightarrow x = 1\}\ \tau_{\ell_0}\ \{at\_\ell_1 \rightarrow x = 1\}$

is not state-valid.

If we use the above heuristic we get

$$pre(\tau_{\ell_0}, \varphi) =$$
$$\forall x', \pi' .\ \underbrace{(move(\ell_0, \ell_1) \wedge x > 0 \wedge x' = x - 1)}_{\rho_{\ell_0}} \rightarrow \underbrace{(at'\_\ell_1 \rightarrow x' = 0)}_{\varphi}$$

Example (cont'd)

$$pre(\tau_{\ell_0}, \varphi) =$$
$$\forall x', \pi' .\ \underbrace{(move(\ell_0, \ell_1) \wedge x > 0 \wedge x' = x - 1)}_{\rho_{\ell_0}} \rightarrow \underbrace{(at'\_\ell_1 \rightarrow x' = 0)}_{\varphi}$$

Since

$$move(\ell_0, \ell_1) \rightarrow at\_\ell_0 \wedge at'\_\ell_1$$
$$x' = x - 1 \wedge x' = 0 \rightarrow x = 1$$

it simplifies to

$$pre(\tau_{\ell_0}, \varphi):\ at\_\ell_0 \wedge x > 0 \rightarrow x = 1$$

Example (cont'd)

$pre(\tau_{\ell_0}, \varphi)$: $at\_\ell_0 \wedge x > 0 \rightarrow x = 1$

Strengthened assertion
$\varphi \wedge pre(\tau_{\ell_0}, \varphi)$: $(at\_\ell_1 \rightarrow x = 0) \wedge (at\_\ell_0 \rightarrow x = 1)$
what we "guessed" before

Show that $\varphi \wedge pre(\tau_{\ell_0}, \varphi)$ is inductive
("strengthening approach")

Simplification of Precondition

Many transition relations have the form

ρ_τ: $C_\tau \wedge \overline{V}' = \overline{E}$

where C_τ is the enabled condition of τ.

And so

$pre(\tau, \varphi)$: $\forall \overline{V}' . C_\tau \wedge \overline{V}' = \overline{E} \rightarrow \varphi'$

can be simplified to

$\forall \overline{V}' . C_\tau \rightarrow \varphi[\overline{E}/\overline{V}]$

replacing all primed variables by its corresponding expression,
thus the quantifier can be eliminated to obtain

$pre(\tau, \varphi)$: $C_\tau \rightarrow \varphi[\overline{E}/\overline{V}]$

Mutual Exclusion for Peterson's Algorithm

local y_1, y_2: boolean where $y_1 = \text{F}, y_2 = \text{F}$
s : integer where $s = 1$

P_1 ::
ℓ_0 : loop forever do
- ℓ_1 : noncritical
- ℓ_2 : $(y_1, s) := (\text{T}, 1)$
- ℓ_3 : await $(\neg y_2) \vee (s = 2)$
- ℓ_4 : critical
- ℓ_5 : $y_1 := \text{F}$

||

P_2 ::
m_0 : loop forever do
- m_1 : noncritical
- m_2 : $(y_2, s) := (\text{T}, 2)$
- m_3 : await $(\neg y_1) \vee (s = 1)$
- m_4 : critical
- m_5 : $y_2 := \text{F}$

Goal:

Mutual Exclusion for Peterson's algorithm:

$$\Box \underbrace{\neg(at\_\ell_4 \wedge at\_m_4)}_{\psi}$$

Bottom-up invariants:

φ_0: $s = 1 \vee s = 2$

φ_1: $y_1 \leftrightarrow at\_\ell_{3..5}$

φ_2: $y_2 \leftrightarrow at\_m_{3..5}$

Example (cont'd)

local y_1, y_2: boolean where $y_1 = \text{F}, y_2 = \text{F}$
s : integer where $s = 1$

P_1 ::
ℓ_0 : loop forever do
- ℓ_1 : noncritical
- ℓ_2 : $(y_1, s) := (\text{T}, 1)$
- ℓ_3 : await $(\neg y_2) \vee (s = 2)$
- ℓ_4 : critical
- ℓ_5 : $y_1 := \text{F}$

||

P_2 ::
m_0 : loop forever do
- m_1 : noncritical
- m_2 : $(y_2, s) := (\text{T}, 2)$
- m_3 : await $(\neg y_1) \vee (s = 1)$
- m_4 : critical
- m_5 : $y_2 := \text{F}$

$$\Box \underbrace{\neg(at\_\ell_4 \wedge at\_m_4)}_{\psi}$$

Problem:

The verification conditions

$\{\varphi_0 \wedge \varphi_1 \wedge \varphi_2 \wedge \psi\}\ \ell_3\ \{\psi\}$

$\{\varphi_0 \wedge \varphi_1 \wedge \varphi_2 \wedge \psi\}\ m_3\ \{\psi\}$

are not state-valid.

Example (cont'd)

$pre(\tau_{\ell_3}, \psi)$: $\forall \pi'$: $\underbrace{move(\ell_3, \ell_4) \wedge (\neg y_2 \vee s \neq 1)}_{\rho_{\ell_3}} \rightarrow$

$$\underbrace{\neg(at'\_\ell_4 \wedge at'\_m_4)}_{\psi'}$$

$pre(\tau_{\ell_3}, \psi)$ simplifies to:

$at\_\ell_3 \wedge (\neg y_2 \vee s \neq 1) \rightarrow \neg at\_m_4$

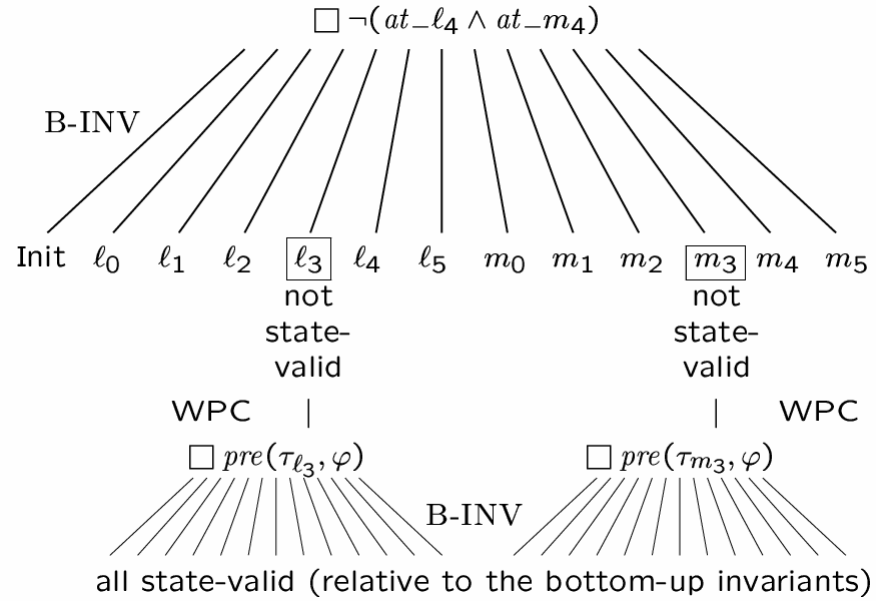
$\boxed{\varphi_3\text{: } at\_\ell_3 \wedge at\_m_4 \rightarrow y_2 \wedge s = 1}$

$pre(\tau_{m_3}, \psi)$: $\forall \pi' \ldots\ldots$

simplifies to:

$\boxed{\varphi_4\text{: } at\_\ell_4 \wedge at\_m_3 \rightarrow y_1 \wedge s = 2}$

Example (cont'd)



Completeness of Rule INV

For assertions q, φ

I1. $P \models \varphi \rightarrow q$

I2. $P \models \Theta \rightarrow \varphi$

I3. $P \models \{\varphi\}\ \mathcal{T}\ \{\varphi\}$

$P \models \Box q$ INV

For every assertion q such that

$\Box q$ is P-valid

there exists an assertion φ such that I1 – I3 are provable from state validities

Note: We actually show *completeness relative to first-order reasoning* taking all state-valid assertions as axioms.

Proof Outline

Given FTS P with system variables

$$\overline{y} = (y_1, \ldots, y_m)$$

- Assume $\Box q$ is P-valid, i.e.,
  (†) q holds over every P-accessible state
- Construct (to be shown) accessibility assertion
  $acc_P(\overline{y})$
  such that for any state s,
  (*) s is P-accessible state iff $s \models acc_P$
- Take $\varphi = acc_P$

We have to show :
1. acc_P satisfies I1 – I3
2. acc_P can be constructed

Proof

1. acc_P satisfies I1 – I3

- Premise I1: $\underbrace{acc_P}_{\varphi} \rightarrow q$

$s \models acc_P \overset{(*)}{\Rightarrow} s$ is P-accessible state

$\overset{(\dagger)}{\Rightarrow} s \models q$

Thus

$\underbrace{acc_P}_{\varphi} \rightarrow q$

is state-valid

Proof (cont'd)

- Premise I2: $\Theta \rightarrow \underbrace{acc_P}_{\varphi}$

$s \models \Theta \Rightarrow s$ is P-accessible

$\overset{(*)}{\Rightarrow} s \models \underbrace{acc_P}_{\varphi}$

Thus

$\Theta \rightarrow \underbrace{acc_P}_{\varphi}$

is state-valid

Proof (cont'd)

- Premise I3: for every $\tau \in \mathcal{T}$,

$$\rho_\tau \wedge acc_P \rightarrow acc'_P$$

where $acc'_P = acc_P(\overline{y}')$.

Take s' to be a $\overline{y}$-variant of s (s agrees with s' on all variables other than $\overline{y}$) and for each y_i take

$$s'[y_i] = s[y'_i]$$

Then

$$\left.\begin{array}{l} s \models \rho_\tau \quad \Rightarrow \quad s' \text{ is a } \tau\text{-successor of } s \\ s \models acc_P \quad \overset{(*)}{\Rightarrow} \quad s \text{ is } P\text{-accessible} \end{array}\right\} \Rightarrow$$

$$\Rightarrow \quad s' \text{ is } P\text{-accessible}$$

$$\overset{(*)}{\Rightarrow} \quad s' \models acc_P$$

$$\Rightarrow \quad s \models acc'_P$$

Proof (cont'd)

2. Construction of acc_P

Assume assertion language includes dynamic array $\underline{a}$ over D

Array $\underline{a}$ is viewed as function,

$$a: [1..n] \mapsto D$$

where n is the size of the array

Assumption is not essential.
E.g., use encoding

$$(n_1, \ldots, n_k) \quad \rightarrow \quad n = p_1^{n_1} \cdots p_k^{n_k}$$

where p_i is the ith prime number

Proof (cont'd)

Case: single-variable y

Define

$acc_P(y)$: $(\exists n > 0)\ \ (\exists a \in [1..n] \mapsto D)\ .\ init \wedge last \wedge evolve$

where

$init$: $\quad \Theta(a[1])$

$last$: $\quad a[n] \ = \ y$

$evolve$: $\quad \forall i\,.\,1 \leq i < n\,.\, \bigvee_{\tau \in \mathcal{T}} \rho_\tau(a[i], a[i{+}1])$

Proof (cont'd)

array a represents a prefix

$$s_1, \ldots, s_n$$

of a computation where $a[i]$ stands for

the value of y at state s_i

Claim:
For any value $d \in D$,

$acc_P(d) = \text{T}$

iff

d is a possible value of y in a P-accessible state

Proof (cont'd)

Multivariable $\overline{y} = (y_1, \ldots, y_m)$ case

Use 2-dimensional array a

y_1		y_m
$a[1,1]$	. . . .	$a[1,m]$
$a[2,1]$	. . . .	$a[2,m]$
.		.
.		.
.		.

Example

V: $\{y\}$	ranges over $\mathbb{Z}$ (the integers)
Θ: $y = 0$	
ρ_τ: $y' = y + 2$	

acc_P: $(\exists n > 0)(\exists a \in [1..n] \mapsto \mathbb{Z})\,.$

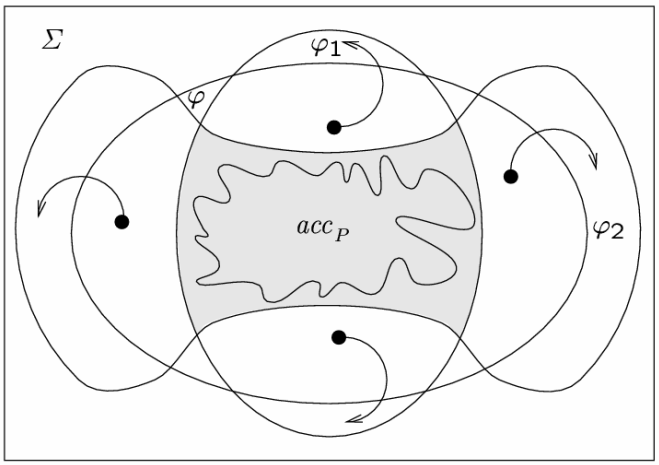
$$\begin{pmatrix} a[1] = 0 \ \wedge \ a[n] = y \ \wedge \\ \forall i\,.\, 1 \le i < n\,.\, a[i+1] = a[i] + 2 \end{pmatrix}$$

simplifies to $(\exists n > 0)(\exists a \in [1..n] \mapsto \mathbb{Z})\,.$

$$\begin{pmatrix} a[n] = y \ \wedge \\ \forall i\,.\, 1 \le i \le n\,.\, a[i] = 2 \cdot (i-1) \end{pmatrix}$$

simplifies to $\boxed{y \ge 0 \ \wedge \ even(y)}$

Discussion



Although the assertion acc_P is inductive and strengthens any P-invariant, it is not very useful in practice.