

LPE Reading Group
24 May 2001

Invariant - some property true at all times

Bank $C \equiv$ initial money

balance : int
account [i] : int $i \in \{0 \dots M\}$

input deposit (m, i)

Eff: balance := balance + m
account [i] := account [i] - m

input withdraw (m, i)

Eff: balance := balance - m
account [i] := account [i] + m

$$\square \left(\sum_{i=1}^M \text{account}[i] + \text{balance} = C \right)$$

P

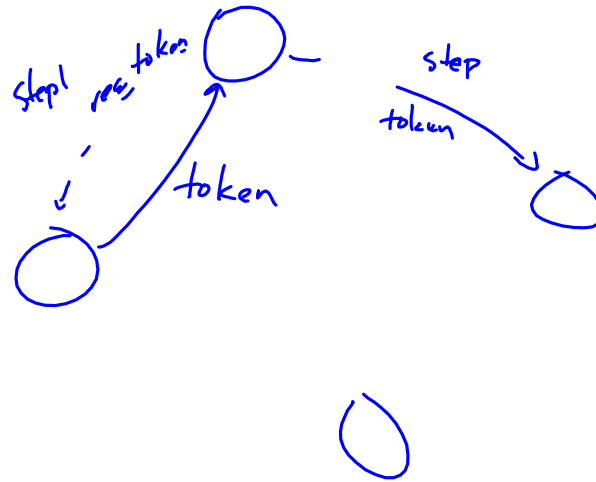
1. Base case

P holds at time 0
(by assumption)

2. Step

P { deposit } P

P remains the same
because balance goes up by m
and account [i] goes down by m



A property P has $\leq P^{-1}r$

a. $\text{sig}(P)$: the set of actions

b. $\text{traces}(P)$: a set of executions

an execution is a sequence of acts($\text{sig}(P)$)

withdraw (\$5, 2)

deposit (\$7, 3)

Verification problem
Given machine A
property P

Show $\text{traces}(A) \subseteq \text{traces}(P)$

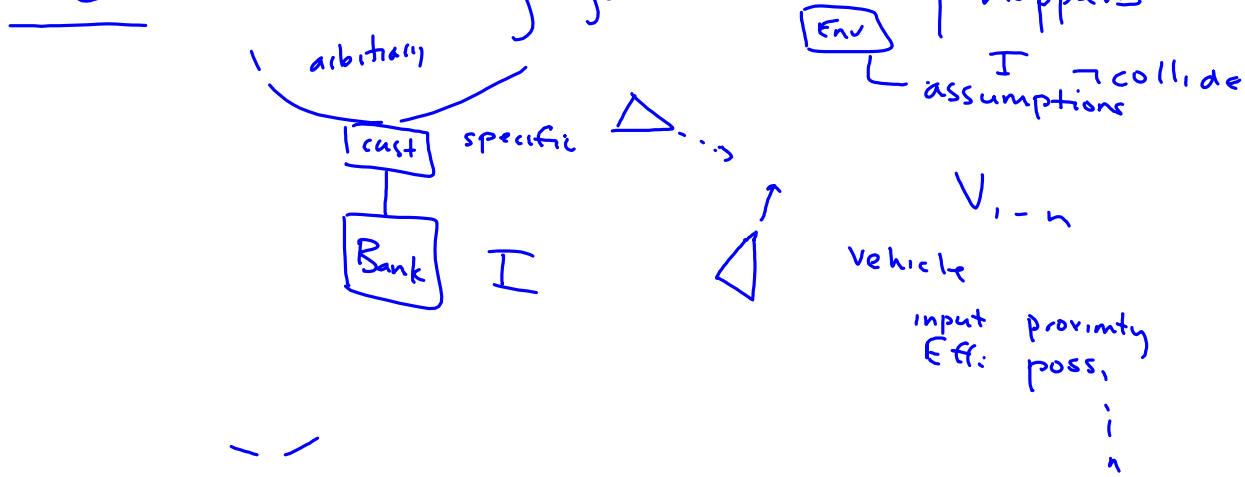
Two kinds of properties

Two kinds of properties:

Safety: nothing "bad" ever happens $B \equiv \text{"bad"}$

$\square \vdash B$

Liveness: something "good" eventually happens



Inv
 $I = \text{"exactly 1 token"}$
 $has_token + |queue| = 1$
 Step send
 $has_token = 1 \wedge |q| = 0$
 after
 $has_token = 0 \wedge |q| = 1$

(Client) \square FIFO
 $has_taken: Bool$
 initially true
 $queue: m\ queue$
 initially empty
 actions
 $send(m)$
 Pre: has_taken
 Eff: $has_taken := false$ Eff: append m to queue
 $recv(m)$
 Pre: m is head of q
 Eff: $remove\ m\ from\ q$
 $tasks ($

Safety: r is a safety property \Rightarrow

a. prefix-closed

$\beta \in \text{traces}(P) \wedge \beta' \leq \beta$ then $\beta' \in \text{traces}(P)$
"prefix"

X b. $\neg \text{traces}(P)$ is nonempty

c. limit-closed

β_1, β_2, \dots infinite seq of finite traces

$\forall i. \beta_i < \beta_{i+1}$

then the limit seq containing all $\beta_i \in \beta$ $\beta \in \text{traces}(P)$

\square I
 \uparrow
 always

Verif

$\text{traces}(A) \subseteq \text{traces}(P)$

Liveness.
 1. if $\beta \in \text{acts}(\text{sig}(P))$
 $\text{act}(P)$ sequence
 then $\exists \beta' \in \text{acts}(P)$ sequence
 "exists"
 s.t.
 $\beta\beta' \in \text{traces}(P)$

Prop includes
 1. sig
 2. a set of traces

A satisfies P
 if $\text{traces}(A) \subseteq \text{traces}(P)$
 $\frac{\text{sig}(P) \quad \text{traces}(P)}{\text{act}(\text{sig}(P))}$

yes - - - - - ∞
 no yes - - - - -
 P no no yes - - - - -
 A FIFO
 $\text{sig} = \{ \text{input send}(m) \quad m \leftarrow \text{output recv}(m) \}$
 A $\text{act} = \{ \text{send}(m), \text{recv}(m) \}$
 $\text{traces} = \text{act sequences}$
 act^*
 $\text{execution} =$
 $S_0 \xrightarrow{a_0} S_1 \xrightarrow{a_1} S_2 \dots$