LPE Reading Group
24 May 2001
Invariant - some property true at all times

Bank

\( C = \text{initial money} \)

\[
\begin{align*}
\text{balance} & : \text{int} \\
\text{account}[i] & : \text{int} \quad i \in \{0, \ldots, M\}
\end{align*}
\]

Input: deposit \((m, i)\)

Eff: \[
\begin{align*}
\text{balance} & := \text{balance} + m \\
\text{account}[i] & := \text{account}[i] - m
\end{align*}
\]

Input: withdraw \((m, i)\)

Eff: \[
\begin{align*}
\text{balance} & := \text{balance} - m \\
\text{account}[i] & := \text{account}[i] + m
\end{align*}
\]

\[
\big \langle \prod_{i=0}^{M} (\text{account}[i] + \text{balance} = C) \big \rangle
\]

1. Base case

\( P \) holds at time 0 (by assumption)

2. Step

\( P \) is deposit \( \exists P \)

\( P \) remains the same because balance goes up by \( m \), and account[i] goes down by \( m \)
A property $P$ nos $= P^{-1}$

- $\text{sig}(P)$: the set of actions
- $\text{traces}(P)$: a set of executions
  
  an execution is a sequence of $\text{acts}(\text{sig}(P))$

 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:
Safety: nothing "bad" ever happens
B = "bad"

Liveness: something "good" eventually happens

arbitrary

specific

Bank

\[ V \text{ in-vehicle} \]

input proximity

Eff. poss.
Inv
I: "exactly 1 token"
has_token + |queue| = 1

Step send
has_token = 1 ∧ |q| = 0

after
has_token = 0 ∧ |q| = 1

Client
has_token: Bool
initially true

FIFO
queue: m queue
initially empty

actions
send (m)

send (true)
Pre: has_token
Eff: has_token := false

recv (m)
Pre: m is head of q
Eff: remove m from q

tasks (}
Safety:  \( S \) is a safety property

1. prefix-closed
   \[ \beta \in \text{traces}(P) \land \beta' \leq \beta \quad \text{then} \quad \beta' \in \text{traces}(P) \]

2. \(-\text{traces}(P)\) is nonempty

3. limit-closed
   \[ \beta, \beta_1, \ldots \quad \text{infinite seq of finite traces} \]
   \[ \forall i. \beta_i < \beta_{i+1} \]
   then the limit seq containing all \( \beta_i \in \mathcal{E} \beta \)
   \[ \beta \in \text{traces}(P) \]
Liveness

1. If $\beta \in \text{act}(p)$ sequence then $\exists \beta' \in \text{act}(p)$ sequence "exists"

s.t. $\beta' \in \text{traces}(p)$

A satisfies P

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

$\text{act}(\text{sig}(p))$

Prop includes

1. $\text{sig}$
2. $\text{a set of traces}$

$\beta$'s include

$\text{act}(\text{sig}(p))$

$\text{FIFO}$

input $\text{send}(m)$, $m \leftarrow \text{output } \text{recv}(m)$

3. $\text{act} = \{ \text{send}(m), \text{recv}(m) \}$

$\text{traces} = \text{act sequences}$

$\text{act}^*$

Execution $\Rightarrow \text{act states}$

So $q_0$, $q_1$, $q_2$, ...