Chapter 1
Invariance: Proof Methods

For assertion $q$ and SPL program $P$
show $P \vDash q$
(i.e., $q$ is $P$-invariant)

**Verification Conditions**
(proof obligations)

**standard verification condition**
For assertions $\varphi, \psi$ and transition $\tau$,

$\{ \varphi \} \tau \{ \psi \}$ ("Hoare triple") stands for the state formula

$$\rho_\tau \land \varphi \rightarrow \psi'$$

"Verification condition (VC) of $\varphi$ and $\psi$
relative to transition $\tau$"

\[ \varphi \quad \tau \quad \psi \]
\[ \downarrow \quad \quad \downarrow \quad \quad \downarrow \]
\[ j \quad \quad \quad j + 1 \]

**Definitions**

Recall:

- the variables of assertion:
  - free (flexible) system variables
    $$V = Y \cup \{ \pi \}$$
    where $Y$ are the program variables and $\pi$ is the control variable
  - quantified (rigid) specification variables

- $q'$ is the primed version of $q$, obtained by replacing each free occurrence of a system variable $y \in V$ by its primed version $y'$.

- $\rho_\tau$ is the transition relation of $\tau$, expressing the relation holding between a state $s$ and any of its $\tau$-successors $s' \in \tau(s)$.
Verification Conditions (Con’t)

- for $\tau \in T$ in $P$
  \[
  \{\varphi\}_{\tau}\{\psi\}: \rho_{\tau} \land \varphi \rightarrow \psi'
  
  "\tau" \text{ leads from } \varphi \text{ to } \psi \text{ in } P"

- for $T$ in $P$
  \[
  \{\varphi\}T\{\psi\}: \{\varphi\}_{\tau}\{\psi\} \text{ for every } \tau \in T
  
  "T" \text{ leads from } \varphi \text{ to } \psi \text{ in } P"

Claim (Verification Condition)
If $\{\varphi\}_{\tau}\{\psi\}$ is $P$-state valid,
then every $\tau$-successor of a $\varphi$-state is a $\psi$-state.

Special Cases

- while, conditional $\rho_{\tau} : \rho_{T} \lor \rho_{F}$
  \[
  \{\varphi\}_{\tau}\{\psi\}: \rho_{T} \land \varphi \rightarrow \psi'
  \[
  \{\varphi\}_{\tau}\{\psi\}: \rho_{F} \land \varphi \rightarrow \psi'

- idle
  \[
  \{\varphi\}_{\tau}\{\psi\}: \rho_{\tau} \land \varphi \rightarrow \varphi'
  
  always valid, since $\rho_{\tau} \rightarrow v' = v$ for all $v \in V$, so $\varphi' = \varphi$.

Verification Conditions (Con’t)
Substituted Form of Verification Condition

Transition relation can be written as

\[
\rho_{\tau} : C_{\tau} \land (\nabla' = E)
\]

where

- $C_{\tau}$: enabling condition
- $\nabla'$: primed variable list
- $E$: expression list

- The substituted form of verification condition $\{\varphi\}_{\tau}\{\psi\}$:
  \[
  [C_{\tau} \land \varphi \rightarrow \psi[E/V]]
  \]
  where
  $\psi[E/V]$:
  replace each variable $v \in \nabla'$ in $\psi$ by the corresponding $e \in E$

Note: No primed variables!

The substituted form of a verification condition is $P$-state valid iff the standard form is valid.

Example:

\[
\rho_{\tau} : x \geq 0 \land y' = x + y \land x' = x
\]
\[
\varphi : y = 3 \quad \psi : y = x + 3
\]

Standard
\[
x \geq 0 \land y' = x + y \land x' = x \land y = 3
\]
\[
\rho_{\tau} \quad \varphi
\]
\[
\rightarrow y' = x' + 3
\]

Substituted
\[
x \geq 0 \land y = 3 \quad \rightarrow x + y = x + 3
\]
\[
C_{\tau} \land \varphi \rightarrow \psi[E/V]
\]
Verification Conditions (Con't)

Example:

\[ \varphi: x = y \quad \psi: x = y + 1 \]

\[ \rho: \frac{x \geq 0}{C} \quad \frac{(x', y')}{V} = \frac{(x + 1, y)}{E} \]

The substituted form of \( \{\varphi\} \tau \{\psi\} \) is

\[ \frac{x \geq 0 \land x = y}{C} \quad \frac{(x = y + 1)[(x + 1, y)/(x, y)]}{\psi[E/V]} \]

or equivalently

\[ x \geq 0 \land x = y \rightarrow x + 1 = y + 1 \]

Proving invariance properties: \( P \vDash \Box q \)

We want to show that for every computation of \( P \)

\[ \sigma: s_0, s_1, s_2, \ldots \]

assertion \( q \) holds in every state \( s_j, j \geq 0 \),

i.e., \( s_j \vDash q \).

Recall:

A sequence \( \sigma: s_0, s_1, s_2, \ldots \) is a computation

if the following hold (from Chapter 0):

1. Initiality: \( s_0 \vDash \Theta \)

2. Consecution: For each \( j \geq 0 \),

\( s_{j+1} \) is a \( \tau \)-successor of \( s_j \) for some \( \tau \in T \)

\( (s_{j+1} \in \tau(s_j)) \)

3, 4. Fairness conditions are respected.

Note: Truth of safety properties over programs does not depend on fairness conditions.

Simplifying Control Expressions

\[ \text{move}(L_1, L_2): \ L_1 \subseteq \pi \land \pi' = (\pi - L_1) \cup L_2 \]

e.g., for \( L_1 = \{\ell_1\}, L_2 = \{\ell_2\} \)

\[ \text{move}(\ell_1, \ell_2): \ \ell_1 \in \pi \land \pi' = (\pi - \{\ell_1\}) \cup \{\ell_2\} \]

Consequences implied by \( \text{move}(L_1, L_2) \):

- for every \([\ell] \in L_1\)

\( \text{at} \_ \ell = \top \) (i.e., \([\ell] \in \pi\))

- for every \([\ell] \in L_2\)

\( \text{at} \_ \ell = \top \) (i.e., \([\ell] \in \pi'\))

- for every \([\ell] \in L_1 - L_2\)

\( \text{at} \_ \ell = \top \) (i.e., \([\ell] \in \pi\)) and

\( \text{at} \_ \ell = \bot \) (i.e., \([\ell] \notin \pi'\))

- for every \( \ell \notin L_1 \cup L_2\)

\( \text{at} \_ \ell = \text{at} \_ \ell \) (i.e., \([\ell] \in \pi, \pi' \) or \([\ell] \notin \pi, \pi'\)

Proving invariance properties (Con't)

This definition suggests a way to prove invariance properties \( \Box q \):

1. Base case:

Prove that \( q \) holds initially

\[ \Theta \rightarrow q \]

i.e., \( q \) holds at \( s_0 \).

2. Inductive step:

prove that \( q \) is preserved by all transitions

\[ q \land \rho \rightarrow q' \]

for all \( \tau \in T \)

\( \{q\} \tau(q) \)

i.e., if \( q \) holds at \( s_j \), then it holds at every \( \tau \)-successor

\( s_{j+1} \).
Rule B-INV (basic invariance)

Show $P \models \Box q$ (i.e. $q$ is $P$-invariant)

For assertion $q$,

B1. $P \models \Theta \rightarrow q$
B2. $P \models \{q\} T \{q\}$

$P \models \Box q$

where B2 stands for $P \models \{q\} \tau \{q\}$ for every $\tau \in T$

- The rule states that if we can prove the $P$-state validity of $\Theta \rightarrow q$ and $\{q\} T \{q\}$, then we can conclude that $\Box q$ is $P$-valid.

- Thus the proof of a temporal property is reduced to the proof of $1 + |T|$ first-order verification conditions.

Example 1: request-release

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

- $\ell_0$: request $x$
- $\ell_1$: critical
- $\ell_2$: release $x$

$\Theta$: $x = 1 \land \pi = \{\ell_0\}$

$T$: $\{\tau_1, \tau_{\ell_0}, \tau_{\ell_1}, \tau_{\ell_2}\}$

Prove $P \models \Box x \geq 0$ using B-INV.

Example 1: request-release (Con't)

B1: $x = 1 \land \pi = \{\ell_0\} \rightarrow x \geq 0$

holds since $x = 1 \rightarrow x \geq 0$

B2:

$\tau_{\ell_0}: \frac{x \geq 0}{q} \land \text{move}(\ell_0, \ell_1) \land x > 0 \land x' = x - 1 \rightarrow \frac{x' \geq 0}{q'}$

holds since $x > 0 \rightarrow x - 1 \geq 0$

$\tau_{\ell_1}: \frac{x \geq 0}{q} \land \text{move}(\ell_1, \ell_2) \land x' = x \rightarrow \frac{x' \geq 0}{q'}$

holds since $x \geq 0 \rightarrow x \geq 0$

$\tau_{\ell_2}: \frac{x \geq 0}{q} \land \text{move}(\ell_2, \ell_3) \land x' = x + 1 \rightarrow \frac{x' \geq 0}{q'}$

holds since $x \geq 0 \rightarrow x + 1 \geq 0$

We proved $P \models \Box x \geq 0$

using B-INV.

Now we want to prove $P \models \Box (at_{\ell_1} \rightarrow x = 0)$
Example 1: request-release (Con’t)

Attempted proof:

B1: \( x = 1 \land \pi = \{\ell_0\} \rightarrow (at_{-\ell_1} \rightarrow x = 0) \)

holds since \( \pi = \{\ell_0\} \rightarrow at_{-\ell_1} = \text{F} \)

B2: \( \{q\} \tau_{\ell_0} \{q\} \)

\[ at_{-\ell_1} \rightarrow x = 0 \land move(\ell_0, \ell_1) \land x > 0 \land x' = x - 1 \]

\[ \rightarrow at'_{-\ell_1} \rightarrow x' = 0 \]

We have \( move(\ell_0, \ell_1) \rightarrow at_{-\ell_1} = \text{F}, \; at'_{-\ell_1} = \text{T} \)

BUT

\( (\text{F} \rightarrow x = 0) \land x > 0 \land x' = x - 1 \rightarrow (\text{T} \rightarrow x' = 0) \)

Cannot prove: not state-valid

What is the problem?
We need a stronger rule.

Strategy 1: Strengthening

Find a stronger assertion \( \varphi \) that is inductive and implies the assertion \( q \) we want to prove.

The problem is:

“The invariant is not inductive”
i.e., it is not strong enough to be preserved by all transitions.

Another way to look at it is to observe that

\( \{q\} \tau_{\ell_0} \{q\} \)

is not state valid, but it is \( P \)-state valid,
i.e., it is true in all \( P \)-accessible states,
since in all \( P \)-accessible states

\( x = 1 \) when at location \( \ell_0 \).

This suggests two strategies to overcome this problem:

• strengthening
• incremental proof

In Chapter 2 it will be shown that there always exists such an assertion \( \varphi \).
Strategy 1: Strengthening (Con't)

Example:

To show
\(\Box (at_{-\ell_1} \rightarrow x = 0)\)

strengthen \(q\) to
\(\varphi: (at_{-\ell_1} \rightarrow x = 0) \land (at_{-\ell_0} \rightarrow x = 1)\)

and show
\(\Box (at_{-\ell_1} \rightarrow x = 0) \land (at_{-\ell_0} \rightarrow x = 1)\)

\(\varphi\)

by rule B-INV.

Strategy 1: Strengthening (Con't)

The strengthening strategy relies on the following rule, MON-I, which, combined with B-INV leads to the general invariance rule INV.

Rule MON-I (Monotonicity)

For assertions \(q_1, q_2\):

\[
\begin{align*}
P \not\vdash \Box q_1 & \quad P \not\vdash q_1 \rightarrow q_2 \\
\hline
P \vdash \Box q_2
\end{align*}
\]

Soundness: If we manage to prove \(\Box q\) using the INV rule for some program \(P\), is \(q\) really an invariant for the program?

We can prove that this is indeed the case. So INV rule is sound.

Completeness: What if \(q\) is an invariant for a program \(P\) but there is no way of proving it under the INV rule?

We can prove that this never happens. There always exists an appropriate \(\varphi\). In other words INV rule is complete.
Strategy 1: Strengthening (Con’t)

Motivation:
\[ P \vdash \Box \varphi \quad \text{(by I2 and I3)} \]
\[ P \not\vdash \varphi \rightarrow q \quad \text{(by I1)} \]
Therefore,
\[ P \vdash \Box q \quad \text{(by MON-1)} \]

i.e., this rule requires that \( \Box \varphi \) holds and \( \varphi \) implies \( q \),
then \( \Box q \) can be concluded to hold by monotonicity.

Control Invariants (Con’t)

- **PARALLEL:**
  for substatement \([S_1||S_2]\):
  \[ \Box (\text{in}_S \leftarrow \text{in}_{S_2}) \]
  i.e., if control is in \( S_1 \) it must also be in \( S_2 \) and vice versa.

Example:
Using the invariant CONFLICT,
\[ \text{move}(\ell_2, \ell_3) \implies l_0 \notin \pi, l_1 \notin \pi, l_3 \notin \pi \]
\[ l_0 \notin \pi', l_1 \notin \pi', l_2 \notin \pi' \]

Strategy 1: Strengthening (Con’t)

We proposed the strengthened invariant
\[ \varphi : (at_{-\ell_0} \rightarrow x = 1) \land (at_{-\ell_1} \rightarrow x = 0) \]
Consider \( \{ \varphi \} \tau_{\ell_0} \{ \varphi \} \):
\[ (at_{-\ell_0} \rightarrow x = 1) \land (at_{-\ell_1} \rightarrow x = 0) \land \varphi \]
\[ \text{move}(\ell_0, \ell_1) \land x > 0 \land x' = x - 1 \]
\[ \vdash (at'_{-\ell_0} \rightarrow x' = 1) \land (at'_{-\ell_1} \rightarrow x' = 0) \land \varphi' \]
\[ \text{move}(\ell_0, \ell_1) \implies \ell_0 \in \pi, \ell_1 \notin \pi, \ell_1 \in \pi', \ell_0 \notin \pi' \]
Therefore
\[ (T \rightarrow x = 1) \land (F \rightarrow \ldots) \land \ldots \land x' = x - 1 \land \ldots \]
\[ \rightarrow (F \rightarrow \ldots) \land (T \rightarrow x' = 0) \]
holds.
Strategy 1: Strengthening (Con’t)

Example (Con’t):
Consider \{\varphi\} \tau_{\ell_2} \{\varphi\}:
\[(at_{-\ell_0} \rightarrow x = 1) \land (at_{-\ell_1} \rightarrow x = 0) \land \varphi'\]
\[move(\ell_2, \ell_3) \land x' = x + 1\]
\[\rightarrow (at'_{-\ell_0} \rightarrow x' = 1) \land (at'_{-\ell_1} \rightarrow x' = 0)\]

\[\varphi'\]
\[move(\ell_2, \ell_3)\] implies \(\ell_3 \in \pi'\)
and by CONFLICT invariants \(\ell_0, \ell_1 \notin \pi'\).

Therefore
\[\ldots \land \ldots \rightarrow (f \rightarrow x' = 1) \land (f \rightarrow x' = 0)\]
holds.

\{\varphi\} \tau_{\ell_2} \{\varphi\} is not state-valid,
but it is \(P\)-state valid. Why?

---

Strategy 2: Incremental proof

Use previously proven invariances \(\chi\) to exclude parts of
the state space from consideration.

\[\Sigma\]
\[\chi\]
\[q\]
\[\tau\]

---

Strategy 2: Incremental proof (Con’t)

Example: (cont’d)

e.g., to show \(\{\chi \land q\} \tau_{\ell_0} \{q\}\), prove
\[(at_{-\ell_0} \rightarrow x = 1) \land (at_{-\ell_1} \rightarrow x = 0) \land \chi\]
\[move(\ell_0, \ell_1) \land x > 0 \land x' = x - 1\]
\[\rightarrow (at'_{-\ell_1} \rightarrow x' = 0)\]

(Example continues...)
Strategy 2: Incremental proof (Con’t)

In an incremental proof we use previously proven properties to eliminate parts of the state space (non $P$-accessible states) from consideration, relying on the following rules:

**Rule SV-PSV**: from state validities to $P$-state validities

For assertions $q_1, q_2$ and $\chi$,

$$P \models \Box \chi \quad P \not\models \chi \land q_1 \rightarrow q_2$$

**Rule i-con**: Conjunction

For assertions $q_1$ and $q_2$,

$$P \not\models \Box q_1 \\
P \not\models \Box q_2$$

$$P \not\models \Box (q_1 \land q_2)$$

---

Example: Program MUX-SEM (mutual exclusion by semaphores)

local $y$: integer where $y = 1$

$$\begin{align*}
P_1 &:: \begin{cases}
\ell_0: \text{loop forever do} \\
\ell_1: \text{noncritical} \\
\ell_2: \text{request } y \\
\ell_3: \text{critical} \\
\ell_4: \text{release } y
\end{cases} \\
P_2 &:: \begin{cases}
m_0: \text{loop forever do} \\
m_1: \text{noncritical} \\
m_2: \text{request } y \\
m_3: \text{critical} \\
m_4: \text{release } y
\end{cases}
\end{align*}$$

Prove mutual exclusion

$\Box \neg (at_{\ell_3} \land at_{m_3})$

---

Program MUX-SEM (Con’t)

3 steps:

$$\Box(y \geq 0)$$

$$\Box(at_{\ell_3,4} + at_{m_3,4} + y = 1)$$

$$\Box \neg (at_{\ell_3} \land at_{m_3})$$

where $F = 0$, $T = 1$.

Let $\pi_\ell$: $\pi \cap \{\ell_0, \ldots, \ell_4\}$

$\pi_m$: $\pi \cap \{m_0, \ldots, m_4\}$

By control invariants (CONFLICT, SOMEWHERE and PARALLEL)

$$|\pi_\ell| = |\pi_m| = 1$$

---

Step 1: $\Box(y \geq 0)$

by rule B-INV

B1. $\pi = \{\ell_0, m_0\} \land y = 1 \rightarrow y \geq 0$

B2. $\rho_r \land y \geq 0 \rightarrow y' \geq 0$

check only $\ell_2, \ell_4, m_2, m_4$

(“$y$-modifiable transitions”)
Program MUX-SEM (Con't)

\( \ell_2: \text{move}(\ell_2, \ell_3) \land y > 0 \land y' = y-1 \land y \geq 0 \)
\[ \phi \]
\[ y' \geq 0 \]
holds since \( y > 0 \rightarrow y-1 \geq 0 \)

\( \ell_4: \text{move}(\ell_4, \ell_0) \land y' = y+1 \land y \geq 0 \rightarrow y' \geq 0 \)
\[ \phi' \]
holds since \( y \geq 0 \rightarrow y+1 \geq 0 \).

Similarly for \( m_2, m_4 \).

Program MUX-SEM (Con't)

Step 2:

\[ \square (at_{-\ell_3,4} + at_{-m_3,4} + y = 1) \]

by rule B-INV

Bl. \( \pi = \{\ell_0, m_0\} \land y = 1 \rightarrow \)
\[ \frac{at_{-\ell_3,4} + at_{-m_3,4} + y = 1}{\phi_2} \]

Program MUX-SEM (Con't)

Step 3: Show \( P \vdash \square \neg (at_{-\ell_3} \land at_{-m_3}) \)

• By i-con

\[ P \vdash \square \phi_1, P \vdash \square \phi_2 \]
\[ P \vdash \square (\phi_1 \land \phi_2) \]
• By mon-i

\[ P \vdash (\phi_1 \land \phi_2) \]
\[ P \vdash \square \frac{y \geq 0}{\phi_1} \land at_{-\ell_3,4} + at_{-m_3,4} + y = 1 \]
\[ \frac{\neg (at_{-\ell_3} \land at_{-m_3})}{\phi_2} \]
\[ P \vdash \square \neg (at_{-\ell_3} \land at_{-m_3}) \]