Axiomatic Derivations

CS 4301/6371: Advanced Programming Languages

Kevin W. Hamlen

April 23, 2024

Axiomatic Derivation Example

$$A \equiv (x = \bar{i} \wedge y = \bar{j})$$
$$B \equiv (x = \max(\bar{i}, \bar{j}) \wedge y = \min(\bar{i}, \bar{j}))$$

$\{A\}$**if** `x <= y` **then** `(x := x + y; y := x - y); x := x - y` **else skip**$\{B\}$

Axiomatic Derivation Example

$$A \equiv (x = \bar{i} \wedge y = \bar{j})$$
$$B \equiv (x = \max(\bar{i}, \bar{j}) \wedge y = \min(\bar{i}, \bar{j}))$$

$$\frac{\{A \wedge x \leq y\}(\texttt{x := x + y; y := x - y});\texttt{x := x - y}\{B\} \qquad \{A \wedge \neg(x \leq y)\}\textbf{skip}\{B\}}{\{A\}\textbf{if}\ \texttt{x <= y}\ \textbf{then}\ (\texttt{x := x + y; y := x - y});\texttt{x := x - y}\ \textbf{else}\ \textbf{skip}\{B\}} \quad (3)$$

Axiomatic Derivation Example

$$A \equiv (x = \bar{i} \wedge y = \bar{j})$$
$$B \equiv (x = \max(\bar{i}, \bar{j}) \wedge y = \min(\bar{i}, \bar{j}))$$

$$\dfrac{\{A \wedge x \le y\}(\mathtt{x := x + y; y := x - y}); \mathtt{x := x - y}\{B\} \qquad \dfrac{\models\ ? \quad \dfrac{}{\{\,?\,\}\mathbf{skip}\{\,?\,\}}(1) \quad \models\ ? \Rightarrow B}{\{A \wedge \neg(x \le y)\}\mathbf{skip}\{B\}}(6)}{\{A\}\mathbf{if}\ \mathtt{x <= y}\ \mathbf{then}\ (\mathtt{x := x + y; y := x - y}); \mathtt{x := x - y}\ \mathbf{else}\ \mathbf{skip}\{B\}}(3)$$

Axiomatic Derivation Example

$$\begin{aligned} A &\equiv (x = \bar{i} \land y = \bar{j}) \\ B &\equiv (x = \max(\bar{i}, \bar{j}) \land y = \min(\bar{i}, \bar{j})) \\ W_1 &\equiv A \land \neg(x \leq y) \Rightarrow B \end{aligned}$$

$$\dfrac{\{A \land x \leq y\}(\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y}\{B\} \qquad \dfrac{\models W_1 \quad \dfrac{}{\{B\}\textbf{skip}\{B\}}(1) \quad \models B \Rightarrow B}{\{A \land \neg(x \leq y)\}\textbf{skip}\{B\}}(6)}{\{A\}\textbf{if}\ \texttt{x<=y}\ \textbf{then}\ (\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y}\ \textbf{else}\ \textbf{skip}\{B\}}(3)$$

Axiomatic Derivation Example

$$A \equiv (x = \bar{i} \wedge y = \bar{j})$$
$$B \equiv (x = \max(\bar{i}, \bar{j}) \wedge y = \min(\bar{i}, \bar{j}))$$
$$W_1 \equiv A \wedge \neg(x \leq y) \Rightarrow B$$

$$\dfrac{\{A \wedge x \leq y\}(\mathtt{x:=x+y;y:=x-y});\mathtt{x:=x-y}\{B\} \qquad \dfrac{\models W_1 \quad \dfrac{}{\{B\}\mathbf{skip}\{B\}}(1) \quad \models B \Rightarrow B}{\{A \wedge \neg(x \leq y)\}\mathbf{skip}\{B\}}(6)}{\{A\}\mathbf{if}\ \mathtt{x <= y}\ \mathbf{then}\ (\mathtt{x:=x+y;y:=x-y});\mathtt{x:=x-y}\ \mathbf{else}\ \mathbf{skip}\{B\}}(3)$$

🤔 Is W_1 universally true?

Axiomatic Derivation Example

$$A \equiv (x = \bar{i} \wedge y = \bar{j})$$
$$B \equiv (x = \max(\bar{i}, \bar{j}) \wedge y = \min(\bar{i}, \bar{j}))$$
$$W_1 \equiv A \wedge \neg(x \le y) \Rightarrow B$$

$$\dfrac{\{A \wedge x \le y\}(\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y}\{B\} \qquad \dfrac{\models W_1 \quad \overline{\{B\}\textbf{skip}\{B\}}^{(1)} \quad \models B \Rightarrow B}{\{A \wedge \neg(x \le y)\}\textbf{skip}\{B\}}(6)}{\{A\}\textbf{if } \texttt{x <= y} \textbf{ then } (\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y} \textbf{ else skip}\{B\}}(3)$$

🤔 Is W_1 universally true?

$(x = \bar{i} \wedge y = \bar{j} \wedge y < x) \Longrightarrow (x = \max(\bar{i}, \bar{j}) \wedge y = \min(\bar{i}, \bar{j}))$ ✅

Axiomatic Derivation Example

$$A \equiv (x = \bar{i} \land y = \bar{j})$$
$$B \equiv (x = \max(\bar{i}, \bar{j}) \land y = \min(\bar{i}, \bar{j}))$$
$$W_1 \equiv A \land \neg(x \le y) \Rightarrow B$$

$$\dfrac{\dfrac{\{A \land x \le y\}\texttt{x:=x+y;y:=x-y}\{\ ?\ \} \qquad \{\ ?\ \}\texttt{x:=x-y}\{B\}}{\{A \land x \le y\}(\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y}\{B\}}(2) \quad \dfrac{\models W_1 \quad \overline{\{B\}\textbf{skip}\{B\}}^{(1)} \quad \models B \Rightarrow B}{\{A \land \neg(x \le y)\}\textbf{skip}\{B\}}(6)}{\{A\}\textbf{if } \texttt{x<=y} \textbf{ then } (\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y} \textbf{ else skip}\{B\}}(3)$$

🤔 Is W_1 universally true?

$(x = \bar{i} \land y = \bar{j} \land y < x) \Longrightarrow (x = \max(\bar{i}, \bar{j}) \land y = \min(\bar{i}, \bar{j}))$ ✅

Axiomatic Derivation Example

$$A \equiv (x = \bar{i} \wedge y = \bar{j})$$
$$B \equiv (x = \max(\bar{i}, \bar{j}) \wedge y = \min(\bar{i}, \bar{j}))$$
$$W_1 \equiv A \wedge \neg(x \le y) \Rightarrow B$$
$$C_1 \equiv B[x - y/x]$$

$$\dfrac{\dfrac{\{A \wedge x \le y\}\texttt{x:=x+y;y:=x-y}\{C_1\} \quad \dfrac{}{\{C_1\}\texttt{x:=x-y}\{B\}}(4)}{\{A \wedge x \le y\}(\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y}\{B\}}(2) \quad \dfrac{\models W_1 \quad \dfrac{}{\{B\}\textbf{skip}\{B\}}(1) \quad \models B \Rightarrow B}{\{A \wedge \neg(x \le y)\}\textbf{skip}\{B\}}(6)}{\{A\}\textbf{if } \texttt{x<=y} \textbf{ then } (\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y} \textbf{ else skip}\{B\}}(3)$$

🤔 Is W_1 universally true?

$$(x = \bar{i} \wedge y = \bar{j} \wedge y < x) \Longrightarrow (x = \max(\bar{i}, \bar{j}) \wedge y = \min(\bar{i}, \bar{j}))$$ ✅

Axiomatic Derivation Example

$$
\begin{aligned}
A &\equiv (x = \bar{i} \wedge y = \bar{j}) \\
B &\equiv (x = \max(\bar{i}, \bar{j}) \wedge y = \min(\bar{i}, \bar{j})) \\
W_1 &\equiv A \wedge \neg(x \leq y) \Rightarrow B \\
C_1 &\equiv B[x - y / x]
\end{aligned}
$$

$$
\dfrac{
\dfrac{
\dfrac{\{A \wedge x \leq y\}\texttt{x:=x+y}\{\ ?\ \} \qquad \{\ ?\ \}\texttt{y:=x-y}\{C_1\}}{\{A \wedge x \leq y\}\texttt{x:=x+y;y:=x-y}\{C_1\}}\,(2)
\qquad
\dfrac{}{\{C_1\}\texttt{x:=x-y}\{B\}}\,(4)
}{\{A \wedge x \leq y\}(\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y}\{B\}}\,(2)
\qquad
\dfrac{\models W_1 \quad \dfrac{}{\{B\}\textbf{skip}\{B\}}\,(1) \quad \models B \Rightarrow B}{\{A \wedge \neg(x \leq y)\}\textbf{skip}\{B\}}\,(6)
}{\{A\}\textbf{if}\ \texttt{x<=y}\ \textbf{then}\ (\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y}\ \textbf{else}\ \textbf{skip}\{B\}}\,(3)
$$

🤔 Is W_1 universally true?

$(x = \bar{i} \wedge y = \bar{j} \wedge y < x) \implies (x = \max(\bar{i}, \bar{j}) \wedge y = \min(\bar{i}, \bar{j}))$ ✅

Axiomatic Derivation Example

$$
\begin{aligned}
A &\equiv (x = \bar{i} \land y = \bar{j}) \\
B &\equiv (x = \max(\bar{i}, \bar{j}) \land y = \min(\bar{i}, \bar{j})) \\
W_1 &\equiv A \land \neg(x \leq y) \Rightarrow B \\
C_1 &\equiv B[x - y/x] \\
C_2 &\equiv C_1[x - y/y]
\end{aligned}
$$

$$
\dfrac{
  \dfrac{
    \dfrac{
      \{A \land x \leq y\}\texttt{x:=x+y}\{C_2\}
      \qquad
      \dfrac{}{\{C_2\}\texttt{y:=x-y}\{C_1\}}\,(4)
    }{
      \{A \land x \leq y\}\texttt{x:=x+y;y:=x-y}\{C_1\}
    }\,(2)
    \qquad
    \dfrac{}{\{C_1\}\texttt{x:=x-y}\{B\}}\,(4)
  }{
    \{A \land x \leq y\}(\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y}\{B\}
  }\,(2)
  \qquad
  \dfrac{
    \models W_1
    \quad
    \dfrac{}{\{B\}\textbf{skip}\{B\}}\,(1)
    \quad
    \models B \Rightarrow B
  }{
    \{A \land \neg(x \leq y)\}\textbf{skip}\{B\}
  }\,(6)
}{
  \{A\}\textbf{if } \texttt{x<=y} \textbf{ then } (\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y} \textbf{ else skip}\{B\}
}\,(3)
$$

🤔 Is W_1 universally true?

$(x = \bar{i} \land y = \bar{j} \land y < x) \Longrightarrow (x = \max(\bar{i}, \bar{j}) \land y = \min(\bar{i}, \bar{j}))$ ✅

Axiomatic Derivation Example

$$A \equiv (x = \bar{i} \land y = \bar{j})$$
$$B \equiv (x = \max(\bar{i}, \bar{j}) \land y = \min(\bar{i}, \bar{j}))$$
$$W_1 \equiv A \land \neg(x \leq y) \Rightarrow B$$
$$C_1 \equiv B[x - y/x]$$
$$C_2 \equiv C_1[x - y/y]$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\{\ ?\ \}\texttt{x:=x+y}\{C_2\}}(4)}{\{A \land x \leq y\}\texttt{x:=x+y}\{C_2\}}(6) \quad \dfrac{}{\{C_2\}\texttt{y:=x-y}\{C_1\}}(4)}{\{A \land x \leq y\}\texttt{x:=x+y;y:=x-y}\{C_1\}}(2) \quad \dfrac{}{\{C_1\}\texttt{x:=x-y}\{B\}}(4)}{\{A \land x \leq y\}(\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y}\{B\}}(2) \quad \dfrac{\models W_1 \quad \dfrac{}{\{B\}\textbf{skip}\{B\}}(1) \quad \models B \Rightarrow B}{\{A \land \neg(x \leq y)\}\textbf{skip}\{B\}}(6)}{\{A\}\textbf{if}\ \texttt{x<=y}\ \textbf{then}\ (\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y}\ \textbf{else}\ \textbf{skip}\{B\}}(3)$$

🤔 Is W_1 universally true?
$(x = \bar{i} \land y = \bar{j} \land y < x) \implies (x = \max(\bar{i}, \bar{j}) \land y = \min(\bar{i}, \bar{j}))$ ✅

Axiomatic Derivation Example

$$
\begin{aligned}
A &\equiv (x = \bar{i} \wedge y = \bar{j}) \\
B &\equiv (x = \max(\bar{i},\bar{j}) \wedge y = \min(\bar{i},\bar{j})) \\
W_1 &\equiv A \wedge \neg(x \le y) \Rightarrow B \\
C_1 &\equiv B[x - y/x] \\
C_2 &\equiv C_1[x - y/y] \\
C_3 &\equiv C_2[x + y/x]
\end{aligned}
$$

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{\models A \wedge x \le y \Rightarrow C_3 \quad \dfrac{}{\{C_3\}\texttt{x:=x+y}\{C_2\}}(4) \quad \models C_2 \Rightarrow C_2}{\{A \wedge x \le y\}\texttt{x:=x+y}\{C_2\}}(6)
\quad
\dfrac{}{\{C_2\}\texttt{y:=x-y}\{C_1\}}(4)
}{\{A \wedge x \le y\}\texttt{x:=x+y;y:=x-y}\{C_1\}}(2)
\quad
\dfrac{}{\{C_1\}\texttt{x:=x-y}\{B\}}(4)
}{\{A \wedge x \le y\}(\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y}\{B\}}(2)
\quad
\dfrac{\models W_1 \quad \dfrac{}{\{B\}\textbf{skip}\{B\}}(1) \quad \models B \Rightarrow B}{\{A \wedge \neg(x \le y)\}\textbf{skip}\{B\}}(6)
}{\{A\}\textbf{if}\ \texttt{x<=y}\ \textbf{then}\ (\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y}\ \textbf{else}\ \textbf{skip}\{B\}}(3)
$$

🤔 Is W_1 universally true?

$$(x = \bar{i} \wedge y = \bar{j} \wedge y < x) \implies (x = \max(\bar{i},\bar{j}) \wedge y = \min(\bar{i},\bar{j}))$$ ✅

Axiomatic Derivation Example

$$
\begin{aligned}
A &\equiv (x = \bar{i} \wedge y = \bar{j}) \\
B &\equiv (x = \max(\bar{i},\bar{j}) \wedge y = \min(\bar{i},\bar{j})) \\
W_1 &\equiv A \wedge \neg(x \leq y) \Rightarrow B \\
C_1 &\equiv B[x-y/x] \\
C_2 &\equiv C_1[x-y/y] \\
C_3 &\equiv C_2[x+y/x]
\end{aligned}
$$

$$
\dfrac{\dfrac{\models A \wedge x \leq y \Rightarrow C_3 \quad \dfrac{}{\{C_3\}\texttt{x:=x+y}\{C_2\}}(4) \quad \models C_2 \Rightarrow C_2}{\{A \wedge x \leq y\}\texttt{x:=x+y}\{C_2\}}(6) \quad \dfrac{}{\{C_2\}\texttt{y:=x-y}\{C_1\}}(4)}{\{A \wedge x \leq y\}\texttt{x:=x+y;y:=x-y}\{C_1\}}(2)
$$

$$
\dfrac{\dfrac{\{A \wedge x \leq y\}\texttt{x:=x+y;y:=x-y}\{C_1\} \quad \dfrac{}{\{C_1\}\texttt{x:=x-y}\{B\}}(4)}{\{A \wedge x \leq y\}(\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y}\{B\}}(2) \quad \dfrac{\models W_1 \quad \dfrac{}{\{B\}\textbf{skip}\{B\}}(1) \quad \models B \Rightarrow B}{\{A \wedge \neg(x \leq y)\}\textbf{skip}\{B\}}(6)}{\{A\}\textbf{if}\ \texttt{x<=y}\ \textbf{then}\ (\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y}\ \textbf{else}\ \textbf{skip}\{B\}}(3)
$$

🤔 Is W_1 universally true?

$$(x = \bar{i} \wedge y = \bar{j} \wedge y < x) \Longrightarrow (x = \max(\bar{i},\bar{j}) \wedge y = \min(\bar{i},\bar{j}))$$ ✅

🤔 Is $A \wedge x \leq y \Rightarrow C_3$ universally true?

Axiomatic Derivation Example

$$
\begin{aligned}
A &\equiv (x = \bar{\imath} \wedge y = \bar{\jmath}) \\
B &\equiv (x = \max(\bar{\imath}, \bar{\jmath}) \wedge y = \min(\bar{\imath}, \bar{\jmath})) \\
W_1 &\equiv A \wedge \neg(x \leq y) \Rightarrow B \\
C_1 &\equiv B[x - y/x] \\
C_2 &\equiv C_1[x - y/y] \\
C_3 &\equiv C_2[x + y/x]
\end{aligned}
$$

$$
\dfrac{\models A \wedge x \leq y \Rightarrow C_3 \qquad \dfrac{}{\{C_3\}\texttt{x:=x+y}\{C_2\}}(4) \qquad \models C_2 \Rightarrow C_2}{\{A \wedge x \leq y\}\texttt{x:=x+y}\{C_2\}}(6)
$$

$$
\dfrac{\{A \wedge x \leq y\}\texttt{x:=x+y}\{C_2\} \qquad \dfrac{}{\{C_2\}\texttt{y:=x-y}\{C_1\}}(4)}{\{A \wedge x \leq y\}\texttt{x:=x+y;y:=x-y}\{C_1\}}(2)
$$

$$
\dfrac{\{A \wedge x \leq y\}\texttt{x:=x+y;y:=x-y}\{C_1\} \qquad \dfrac{}{\{C_1\}\texttt{x:=x-y}\{B\}}(4)}{\{A \wedge x \leq y\}(\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y}\{B\}}(2)
$$

$$
\dfrac{\models W_1 \qquad \dfrac{}{\{B\}\textbf{skip}\{B\}}(1) \qquad \models B \Rightarrow B}{\{A \wedge \neg(x \leq y)\}\textbf{skip}\{B\}}(6)
$$

$$
\dfrac{\{A \wedge x \leq y\}(\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y}\{B\} \qquad \{A \wedge \neg(x \leq y)\}\textbf{skip}\{B\}}{\{A\}\textbf{if } \texttt{x <= y} \textbf{ then } (\texttt{x:=x+y;y:=x-y});\texttt{x:=x-y} \textbf{ else skip}\{B\}}(3)
$$

🤔 Is W_1 universally true?

$$(x = \bar{\imath} \wedge y = \bar{\jmath} \wedge y < x) \Longrightarrow (x = \max(\bar{\imath}, \bar{\jmath}) \wedge y = \min(\bar{\imath}, \bar{\jmath}))$$ ✅

🤔 Is $A \wedge x \leq y \Rightarrow C_3$ universally true?

$$
\begin{aligned}
C_3 &\equiv C_2[x + y] \equiv C_1[x - y/y][x + y/x] \equiv B[x - y/x][x - y/y][x + y/x] \\
&\equiv (x + y) - ((x + y) - y) = \max(\bar{\imath}, \bar{\jmath}) \wedge (x + y) - y = \min(\bar{\imath}, \bar{\jmath}) \\
&\equiv y = \max(\bar{\imath}, \bar{\jmath}) \wedge x = \min(\bar{\imath}, \bar{\jmath})
\end{aligned}
$$

$$(x = \bar{\imath} \wedge y = \bar{\jmath} \wedge x \leq y) \Longrightarrow (y = \max(\bar{\imath}, \bar{\jmath}) \wedge x = \min(\bar{\imath}, \bar{\jmath}))$$ ✅

Building Axiomatic Derivations

- Work bottom-up, right-to-left.
- Never use the Rule of Consequence (6) unless no other rule applies.
  - Never use the Rule of Consequence more than once consecutively.
- When using Rule of Consequence, double-check its premises are universally true (and show work for partial credit).
  - No need to show explicit derivations for models premises, though.
- Each rule must be applied verbatim.
  - No simplifications of expressions, no rearrangement of conjuncts, no renaming of variables, etc.
  - But you may define and use abbreviations (e.g., $A \equiv \ldots$) to shorten writing.
  - Simplifications and rearrangements of terms are for Rule of Consequence.
- With this procedure your derivation-building process should be essentially deterministic (no choices) except for while-loops.

While Loops

- Proving correctness of loops is the hard part.
  - Distills down to one central problem: What is the loop invariant?
  - This is the central challenge for almost all program verification.
- Illustration by example (next slide)

Example of While-loop Verification

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A}\underbrace{\texttt{while}\ \overbrace{1\ \texttt{<=}\ \texttt{x}}^{b}\ \texttt{do}\ \overbrace{(\texttt{y:=y+x;x:=x-}1)}^{c}}_{w}\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$\{A\}w\{B\}$$

Example of While-loop Verification

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A}\underbrace{\texttt{while}\ \overbrace{1\ \texttt{<=}\ \texttt{x}}^{b}\ \texttt{do}\ \overbrace{(\texttt{y:=y+x;x:=x-}1)}^{c}}_{w}\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$\frac{\models A \Rightarrow I \qquad \dfrac{\{I \wedge b\}c\{I\}}{\{I\}w\{\neg b \wedge I\}}(5) \qquad \models (\neg b \wedge I) \Rightarrow B}{\{A\}w\{B\}}(6)$$

Example of While-loop Verification

$$\underbrace{\{x = \bar{i} \land 1 \leq \bar{i} \land y = 0\}}_{A}\underbrace{\texttt{while}\ \overbrace{\texttt{1 <= x}}^{b}\ \texttt{do}\ \overbrace{(\texttt{y := y + x ; x := x - 1})}^{c}}_{w}\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$\cfrac{\models A \Rightarrow I \qquad \cfrac{\cfrac{\{I \land b\}\texttt{y := y + x}\{\ ?\ \} \qquad \{\ ?\ \}\texttt{x := x - 1}\{I\}}{\{I \land b\}c\{I\}}\text{(2)}}{\{I\}w\{\neg b \land I\}}\text{(5)} \qquad \models (\neg b \land I) \Rightarrow B}{\{A\}w\{B\}}\text{(6)}$$

Example of While-loop Verification

$$\underbrace{\{x = \bar{i} \land 1 \leq \bar{i} \land y = 0\}}_{A}\underbrace{\textbf{while}\ \overbrace{1 \mathtt{<=} \mathtt{x}}^{b}\ \textbf{do}\ \overbrace{(\mathtt{y := y + x ; x := x - 1})}^{c}}_{w}\underbrace{\{y = \bar{i}(\bar{i} + 1)/2\}}_{B}$$

$$I \equiv ?$$
$$C \equiv I[x - 1/x]$$

$$\dfrac{\models A \Rightarrow I \qquad \dfrac{\dfrac{\{I \land b\}\mathtt{y := y + x}\{C\} \qquad \dfrac{}{\{C\}\mathtt{x := x - 1}\{I\}}(4)}{\{I \land b\}c\{I\}}(2)}{\{I\}w\{\neg b \land I\}}(5) \qquad \models (\neg b \land I) \Rightarrow B}{\{A\}w\{B\}}(6)$$

Example of While-loop Verification

$$\underbrace{\{x = \bar{i} \land 1 \leq \bar{i} \land y = 0\}}_{A}\underbrace{\texttt{while}\ \overbrace{\texttt{1 <= x}}^{b}\ \texttt{do}\ \overbrace{(\texttt{y:=y+x;x:=x-1})}^{c}}_{w}\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$
$$C \equiv I[x-1/x]$$

$$\dfrac{\models A \Rightarrow I \qquad \dfrac{\dfrac{\dfrac{\models I \land b \Rightarrow ? \quad \{?\}\texttt{y:=y+x}\{?\} \quad \models ? \Rightarrow C}{\{I \land b\}\texttt{y:=y+x}\{C\}}(6) \qquad \dfrac{}{\{C\}\texttt{x:=x-1}\{I\}}(4)}{\{I \land b\}c\{I\}}(2)}{\{I\}w\{\neg b \land I\}}(5) \qquad \models (\neg b \land I) \Rightarrow B}{\{A\}w\{B\}}(6)$$

Example of While-loop Verification

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A}\underbrace{\texttt{while}\ \overbrace{\texttt{1 <= x}}^{b}\ \texttt{do}\ \overbrace{(\texttt{y := y + x ; x := x - 1})}^{c}}_{w}\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$
$$C \equiv I[x-1/x]$$

$$\dfrac{\models A \Rightarrow I \qquad \dfrac{\dfrac{\dfrac{\models I \wedge b \Rightarrow ? \qquad \dfrac{}{\{\,?\,\}\texttt{y := y + x}\{C\}}(4) \qquad \models C \Rightarrow C}{\{I \wedge b\}\texttt{y := y + x}\{C\}}(6) \qquad \dfrac{}{\{C\}\texttt{x := x - 1}\{I\}}(4)}{\{I \wedge b\}c\{I\}}(2)}{\{I\}w\{\neg b \wedge I\}}(5) \qquad \models (\neg b \wedge I) \Rightarrow B}{\{A\}w\{B\}}(6)$$

Example of While-loop Verification

$$\underbrace{\{x = \bar{i} \wedge 1 \le \bar{i} \wedge y = 0\}}_{A}\underbrace{\texttt{while}\ \overbrace{\texttt{1 <= x}}^{b}\ \texttt{do}\ \overbrace{(\texttt{y := y + x ; x := x - 1})}^{c}}_{w}\underbrace{\{y = \bar{i}(\bar{i} + 1)/2\}}_{B}$$

$$\begin{aligned} I &\equiv ? \\ C &\equiv I[x - 1/x] \\ I' &\equiv C[y + x/y] \end{aligned}$$

$$\dfrac{\models A \Rightarrow I \qquad \dfrac{\dfrac{\dfrac{\models I \wedge b \Rightarrow I' \quad \dfrac{}{\{I'\}\texttt{y := y + x}\{C\}}(4) \quad \models C \Rightarrow C}{\{I \wedge b\}\texttt{y := y + x}\{C\}}(6) \quad \dfrac{}{\{C\}\texttt{x := x - 1}\{I\}}(4)}{\{I \wedge b\}c\{I\}}(2)}{\{I\}w\{\neg b \wedge I\}}(5) \qquad \models (\neg b \wedge I) \Rightarrow B}{\{A\}w\{B\}}(6)$$

Example of While-loop Verification

$$\underbrace{\{x = \bar{i} \land 1 \leq \bar{i} \land y = 0\}}_{A}\underbrace{\texttt{while}\ \overbrace{\texttt{1 <= x}}^{b}\ \texttt{do}\ \overbrace{(\texttt{y := y + x ; x := x - 1})}^{c}}_{w}\underbrace{\{y = \bar{i}(\bar{i} + 1)/2\}}_{B}$$

$$\begin{aligned} I &\equiv ? \\ C &\equiv I[x - 1/x] \\ I' &\equiv C[y + x/y] \end{aligned}$$

$$\dfrac{\overset{❶}{\models A \Rightarrow I} \quad \dfrac{\dfrac{\dfrac{\overset{❷}{\models I \land b \Rightarrow I'} \quad \dfrac{}{\{I'\}\texttt{y := y + x}\{C\}}(4) \quad \models C \Rightarrow C}{\{I \land b\}\texttt{y := y + x}\{C\}}(6) \quad \dfrac{}{\{C\}\texttt{x := x - 1}\{I\}}(4)}{\{I \land b\}c\{I\}}(2)}{\{I\}w\{\neg b \land I\}}(5) \quad \overset{❸}{\models (\neg b \land I) \Rightarrow B}}{\{A\}w\{B\}}(6)$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A}\textbf{while } 1 \texttt{ <= x } \textbf{do } (\texttt{y := y + x ; x := x - } 1)\underbrace{\{y = \bar{i}(\bar{i} + 1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x - 1/x][y + x/y]$$

1. $\models A \Rightarrow I$ — The precondition must imply the invariant.
2. $\models I \wedge b \Rightarrow I'$ — The invariant must be preserved by each loop iteration.
3. $\models (\neg b \wedge I) \Rightarrow B$ — The invariant with the loop termination condition must be enough to prove the postcondition.

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A}\textbf{while } 1 \texttt{ <= x } \textbf{do } (\texttt{y := y + x ; x := x - } 1)\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x - 1/x][y + x/y]$$

1. $\models A \Rightarrow I$ — The precondition must imply the invariant.
2. $\models I \wedge b \Rightarrow I'$ — The invariant must be preserved by each loop iteration.
3. $\models (\neg b \wedge I) \Rightarrow B$ — The invariant with the loop termination condition must be enough to prove the postcondition.

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A}\ \textbf{while}\ 1\ \texttt{<=}\ \texttt{x}\ \textbf{do}\ (\texttt{y := y + x; x := x - 1})\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

❶ $\models A \Rightarrow I$ — The precondition must imply the invariant.

❷ $\models I \wedge b \Rightarrow I'$ — The invariant must be preserved by each loop iteration.

❸ $\models (\neg b \wedge I) \Rightarrow B$ — The invariant with the loop termination condition must be enough to prove the postcondition.

$$\neg(1 \leq x) \wedge y = \bar{i}(\bar{i}+1)/2 \Rightarrow y = \bar{i}(\bar{i}+1)/2$$

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A}\texttt{while } 1 \texttt{ <= x do } (\texttt{y := y + x; x := x - } 1)\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

1. $\models A \Rightarrow I$ — The precondition must imply the invariant.
2. $\models I \wedge b \Rightarrow I'$ — The invariant must be preserved by each loop iteration.
3. $\models (\neg b \wedge I) \Rightarrow B$ — The invariant with the loop termination condition must be enough to prove the postcondition.

$$\neg(1 \leq x) \wedge y = \bar{i}(\bar{i}+1)/2 \Rightarrow y = \bar{i}(\bar{i}+1)/2 \ ✅$$

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \wedge 1 \le \bar{i} \wedge y = 0\}}_{A} \texttt{while } 1 \texttt{ <= x do } (\texttt{y := y + x ; x := x - } 1) \underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

1. $\models A \Rightarrow I$ — The precondition must imply the invariant. $\quad x = \bar{i} \wedge 1 \le \bar{i} \wedge y = 0 \Rightarrow y = \bar{i}(\bar{i}+1)/2$
2. $\models I \wedge b \Rightarrow I'$ — The invariant must be preserved by each loop iteration.
3. $\models (\neg b \wedge I) \Rightarrow B$ — The invariant with the loop termination condition must be enough to prove the postcondition. $\quad \neg(1 \le x) \wedge y = \bar{i}(\bar{i}+1)/2 \Rightarrow y = \bar{i}(\bar{i}+1)/2$ ✅

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \land 1 \leq \bar{i} \land y = 0\}}_{A}\texttt{while } 1 \texttt{ <= x do } (\texttt{y := y + x; x := x - } 1)\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

1. $\models A \Rightarrow I$ — The precondition must imply the invariant. — $x = \bar{i} \land 1 \leq \bar{i} \land y = 0 \Rightarrow y = \bar{i}(\bar{i}+1)/2$ ✗
2. $\models I \land b \Rightarrow I'$ — The invariant must be preserved by each loop iteration.
3. $\models (\neg b \land I) \Rightarrow B$ — The invariant with the loop termination condition must be enough to prove the postcondition. — $\neg(1 \leq x) \land y = \bar{i}(\bar{i}+1)/2 \Rightarrow y = \bar{i}(\bar{i}+1)/2$ ✅

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A}\ \texttt{while}\ 1 \texttt{<=} \texttt{x}\ \texttt{do}\ (\texttt{y:=y+x;x:=x-1})\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

1. $\models A \Rightarrow I$ — The precondition must imply the invariant. — $x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0 \Rightarrow y = \bar{i}(\bar{i}+1)/2$ ✗
2. $\models I \wedge b \Rightarrow I'$ — The invariant must be preserved by each loop iteration. — $y = \bar{i}(\bar{i}+1)/2 \wedge 1 \leq x \Rightarrow y + x = \bar{i}(\bar{i}+1)/2$
3. $\models (\neg b \wedge I) \Rightarrow B$ — The invariant with the loop termination condition must be enough to prove the postcondition. — $\neg(1 \leq x) \wedge y = \bar{i}(\bar{i}+1)/2 \Rightarrow y = \bar{i}(\bar{i}+1)/2$ ✅

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \wedge 1 \le \bar{i} \wedge y = 0\}}_{A}\ \texttt{while}\ 1\ \texttt{<=}\ \texttt{x}\ \texttt{do}\ (\texttt{y:=y+x;x:=x-1})\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

1. $\models A \Rightarrow I$ — The precondition must imply the invariant. — $x = \bar{i} \wedge 1 \le \bar{i} \wedge y = 0 \Rightarrow y = \bar{i}(\bar{i}+1)/2$ ✗
2. $\models I \wedge b \Rightarrow I'$ — The invariant must be preserved by each loop iteration. — $y = \bar{i}(\bar{i}+1)/2 \wedge 1 \le x \Rightarrow y + x = \bar{i}(\bar{i}+1)/2$ ✗
3. $\models (\neg b \wedge I) \Rightarrow B$ — The invariant with the loop termination condition must be enough to prove the postcondition. — $\neg(1 \le x) \wedge y = \bar{i}(\bar{i}+1)/2 \Rightarrow y = \bar{i}(\bar{i}+1)/2$ ✅

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A}\ \texttt{while}\ 1 \ \texttt{<=}\ \texttt{x}\ \texttt{do}\ (\texttt{y := y + x ; x := x - 1})\ \underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

1. $\models A \Rightarrow I$ — The precondition must imply the invariant.
2. $\models I \wedge b \Rightarrow I'$ — The invariant must be preserved by each loop iteration.
3. $\models (\neg b \wedge I) \Rightarrow B$ — The invariant with the loop termination condition must be enough to prove the postcondition.

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A}\ \texttt{while}\ 1\ \texttt{<=}\ \texttt{x}\ \texttt{do}\ (\texttt{y:=y+x;x:=x-1})\ \underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

1. $\models A \Rightarrow I$ — The precondition must imply the invariant.
2. $\models I \wedge b \Rightarrow I'$ — The invariant must be preserved by each loop iteration.
3. $\models (\neg b \wedge I) \Rightarrow B$ — The invariant with the loop termination condition must be enough to prove the postcondition.

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2 - (x-1)(x-1+1)/2$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A}\,\textbf{while}\ 1\ \texttt{<=}\ \texttt{x}\ \textbf{do}\ (\texttt{y := y + x ; x := x - 1})\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

1. $\models A \Rightarrow I$ — The precondition must imply the invariant.

   $x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0 \Rightarrow y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2$

2. $\models I \wedge b \Rightarrow I'$ — The invariant must be preserved by each loop iteration.

3. $\models (\neg b \wedge I) \Rightarrow B$ — The invariant with the loop termination condition must be enough to prove the postcondition.

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2 - (x-1)(x-1+1)/2$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A}\ \mathbf{while}\ 1 \texttt{<=} \texttt{x}\ \mathbf{do}\ (\texttt{y:=y+x;x:=x-}1)\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

1. $\models A \Rightarrow I$ — The precondition must imply the invariant.
2. $\models I \wedge b \Rightarrow I'$ — The invariant must be preserved by each loop iteration.
3. $\models (\neg b \wedge I) \Rightarrow B$ — The invariant with the loop termination condition must be enough to prove the postcondition.

$$x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0$$
$$\Rightarrow y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \ ✅$$

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2 - (x-1)(x-1+1)/2$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \land 1 \leq \bar{i} \land y = 0\}}_{A}\ \textbf{while}\ 1 \texttt{<=} \texttt{x}\ \textbf{do}\ (\texttt{y := y + x ; x := x - 1})\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

1. $\models A \Rightarrow I$ — The precondition must imply the invariant.
   $x = \bar{i} \land 1 \leq \bar{i} \land y = 0$
   $\Rightarrow y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2$ ✅
2. $\models I \land b \Rightarrow I'$ — The invariant must be preserved by each loop iteration.
   $y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \land 1 \leq x$
   $\Rightarrow y + x = \bar{i}(\bar{i}+1)/2 - (x-1)x/2$
3. $\models (\neg b \land I) \Rightarrow B$ — The invariant with the loop termination condition must be enough to prove the postcondition.

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2 - (x-1)(x-1+1)/2$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \land 1 \leq \bar{i} \land y = 0\}}_{A}\ \mathbf{while}\ 1 \texttt{ <= x } \mathbf{do}\ (\texttt{y := y + x ; x := x - } 1)\ \underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

1. $\models A \Rightarrow I$ — The precondition must imply the invariant.
   $x = \bar{i} \land 1 \leq \bar{i} \land y = 0 \Rightarrow y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2$ ✅
2. $\models I \land b \Rightarrow I'$ — The invariant must be preserved by each loop iteration.
   $y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \land 1 \leq x \Rightarrow y + x = \bar{i}(\bar{i}+1)/2 - (x-1)x/2$ ✅
3. $\models (\neg b \land I) \Rightarrow B$ — The invariant with the loop termination condition must be enough to prove the postcondition.

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2 - (x-1)(x-1+1)/2$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A}\ \textbf{while}\ 1 \texttt{ <= x }\ \textbf{do}\ (\texttt{y := y + x ; x := x - } 1)\ \underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

❶ $\models A \Rightarrow I$	The precondition must imply the invariant.	$x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0 \Rightarrow y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2$ ✅
❷ $\models I \wedge b \Rightarrow I'$	The invariant must be preserved by each loop iteration.	$y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \wedge 1 \leq x \Rightarrow y + x = \bar{i}(\bar{i}+1)/2 - (x-1)x/2$ ✅
❸ $\models (\neg b \wedge I) \Rightarrow B$	The invariant with the loop termination condition must be enough to prove the postcondition.	$\neg(1 \leq x) \wedge y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \Rightarrow y = \bar{i}(\bar{i}+1)/2$

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2 - (x-1)(x-1+1)/2$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A}\texttt{while } 1 \texttt{ <= x do } (\texttt{y:=y+x;x:=x-}1)\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

❶ $\models A \Rightarrow I$ — The precondition must imply the invariant.

$x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0 \Rightarrow y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2$ ✅

❷ $\models I \wedge b \Rightarrow I'$ — The invariant must be preserved by each loop iteration.

$y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \wedge 1 \leq x \Rightarrow y + x = \bar{i}(\bar{i}+1)/2 - (x-1)x/2$ ✅

❸ $\models (\neg b \wedge I) \Rightarrow B$ — The invariant with the loop termination condition must be enough to prove the postcondition.

$\neg(1 \leq x) \wedge y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \Rightarrow y = \bar{i}(\bar{i}+1)/2$ ❌

counter-example: $x = -10,\ y = 0,\ \bar{i} = 9$

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2 - (x-1)(x-1+1)/2$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A}\texttt{while } 1 \texttt{ <= x do } (\texttt{y := y + x ; x := x - } 1)\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x - 1/x][y + x/y]$$

1. $\models A \Rightarrow I$ — The precondition must imply the invariant. $x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0 \Rightarrow y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2$ ✅
2. $\models I \wedge b \Rightarrow I'$ — The invariant must be preserved by each loop iteration. $y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \wedge 1 \leq x \Rightarrow y + x = \bar{i}(\bar{i}+1)/2 - (x-1)x/2$ ✅
3. $\models (\neg b \wedge I) \Rightarrow B$ — The invariant with the loop termination condition must be enough to prove the postcondition. $\neg(1 \leq x) \wedge y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \Rightarrow y = \bar{i}(\bar{i}+1)/2$ ❌
   counter-example: $x = -10,\ y = 0,\ \bar{i} = 9$

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \wedge 0 \leq x$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2 - (x-1)(x-1+1)/2$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A}\textbf{while } 1 \texttt{<=} \texttt{x} \textbf{ do } (\texttt{y:=y+x;x:=x-}1)\underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

❶ $\models A \Rightarrow I$

$$x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0$$
$$\Rightarrow y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \wedge 0 \leq x$$

❷ $\models I \wedge b \Rightarrow I'$

$$y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \wedge 1 \leq x \wedge 0 \leq x$$
$$\Rightarrow y + x = \bar{i}(\bar{i}+1)/2 - (x-1)x/2 \wedge 0 \leq x - 1$$

❸ $\models (\neg b \wedge I) \Rightarrow B$

$$\neg(1 \leq x) \wedge y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \wedge 0 \leq x$$
$$\Rightarrow y = \bar{i}(\bar{i}+1)/2$$

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \wedge 0 \leq x$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2 - (x-1)(x-1+1)/2 \wedge 0 \leq x - 1$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \land 1 \leq \bar{i} \land y = 0\}}_{A} \textbf{while } 1 \texttt{ <= x } \textbf{do } (\texttt{y := y + x ; x := x - } 1) \underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

❶ $\models A \Rightarrow I$

$$x = \bar{i} \land 1 \leq \bar{i} \land y = 0$$
$$\Rightarrow y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \land 0 \leq x \checkmark$$

❷ $\models I \land b \Rightarrow I'$

$$y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \land 1 \leq x \land 0 \leq x$$
$$\Rightarrow y + x = \bar{i}(\bar{i}+1)/2 - (x-1)x/2 \land 0 \leq x - 1$$

❸ $\models (\neg b \land I) \Rightarrow B$

$$\neg(1 \leq x) \land y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \land 0 \leq x$$
$$\Rightarrow y = \bar{i}(\bar{i}+1)/2$$

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \land 0 \leq x$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2 - (x-1)(x-1+1)/2 \land 0 \leq x - 1$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0\}}_{A} \texttt{while } 1 \texttt{ <= x do } (\texttt{y := y + x ; x := x - }1) \underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

❶ $\models A \Rightarrow I$

$$x = \bar{i} \wedge 1 \leq \bar{i} \wedge y = 0$$
$$\Rightarrow y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \wedge 0 \leq x \text{ ✅}$$

❷ $\models I \wedge b \Rightarrow I'$

$$y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \wedge 1 \leq x \wedge 0 \leq x$$
$$\Rightarrow y + x = \bar{i}(\bar{i}+1)/2 - (x-1)x/2 \wedge 0 \leq x - 1 \text{ ✅}$$

❸ $\models (\neg b \wedge I) \Rightarrow B$

$$\neg(1 \leq x) \wedge y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \wedge 0 \leq x$$
$$\Rightarrow y = \bar{i}(\bar{i}+1)/2$$

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \wedge 0 \leq x$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2 - (x-1)(x-1+1)/2 \wedge 0 \leq x - 1$$

Finding the Loop Invariant

$$\underbrace{\{x = \bar{i} \land 1 \leq \bar{i} \land y = 0\}}_{A}\ \mathbf{while}\ 1\ \texttt{<=}\ \texttt{x}\ \mathbf{do}\ (\texttt{y := y + x ; x := x - 1})\ \underbrace{\{y = \bar{i}(\bar{i}+1)/2\}}_{B}$$

$$I \equiv ?$$

$$I' \equiv I[x-1/x][y+x/y]$$

❶ $\models A \Rightarrow I$

$$x = \bar{i} \land 1 \leq \bar{i} \land y = 0$$
$$\Rightarrow y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \land 0 \leq x \ ✅$$

❷ $\models I \land b \Rightarrow I'$

$$y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \land 1 \leq x \land 0 \leq x$$
$$\Rightarrow y + x = \bar{i}(\bar{i}+1)/2 - (x-1)x/2 \land 0 \leq x - 1 \ ✅$$

❸ $\models (\neg b \land I) \Rightarrow B$

$$\neg(1 \leq x) \land y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \land 0 \leq x$$
$$\Rightarrow y = \bar{i}(\bar{i}+1)/2 \ ✅$$

Example: Try $I \equiv y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2 \land 0 \leq x$

$$I' \equiv y + x = \bar{i}(\bar{i}+1)/2 - (x-1)(x-1+1)/2 \land 0 \leq x - 1$$

Two Kinds of Invariant Failure

- When ❸ fails...
  - Invariant is too weak to prove the postcondition.
  - Need more/better information to know that loop computes correct results.
- When ❶ and/or ❷ fails...
  - Invariant is not even true (on every iteration)!
  - Can be thought of as being "too strong" (asserts things so powerful that they're not true)
- Extreme cases:
  - $I = T$ (weakest possible invariant) guaranteed to satisfy ❶ and ❷
  - $I = F$ (strongest possible invariant) guaranteed to satisfy ❸
  - $I = B$ (postcondition) also guaranteed to satisfy ❸ but almost never ❶ or ❷

Tips for Finding Good Loop Invariants

- There is no magic procedure for finding a good invariant.
  - Need to understand *why* the program works
  - Think of a statement that's true before and after every iteration, and that somehow captures the "progress" that the loop is making toward a solution.
- Check whether your invariant satisfies the three criteria(!!!)
  - Really do the algebra; don't just guess that it seems true.
  - Don't use your knowledge of the loop when checking! Criteria must be *universally true* (i.e., pure algebraic proof with no appeal to code).
  - Identifying where criteria succeed and fail is worth significant partial credit.
- Many correct invariants consist of two pieces:
  1. "main part" captures loop's "progress" (e.g., $y = \bar{i}(\bar{i}+1)/2 - x(x+1)/2$)
  2. "boundary conditions" limit variable values (e.g., $0 \leq x$)
- Never introduce new, unquantified (meta-)variables in your invariant.
  - Example: Never define "$I \equiv \ldots n \ldots$ where n is the number of loop iterations so far."
  - Reason: Program does not "know" how many iterations so far. Somehow it is correct without tracking that.