



Verification conditions:

Adequacy: Pre \Rightarrow A₁, A₈ \Rightarrow Post

Inductive:

$$\begin{aligned}
 &\{(x \geq 0 \wedge y > 0 \wedge q' = 0) \Rightarrow A_2\} \wedge \\
 &\{(x \geq 0 \wedge y > 0 \wedge q = 0 \wedge r' = x) \Rightarrow A_3\} \wedge \\
 &\{(x \geq 0 \wedge y > 0 \wedge q = 0 \wedge r = x) \Rightarrow A_4\} \wedge \\
 &\{(x \geq 0 \wedge y > 0 \wedge x = qy + r \wedge r \geq y) \Rightarrow A_5\} \wedge \\
 &\{(x \geq 0 \wedge y > 0 \wedge r' = r - y \wedge x' = qy + y + r - y) \Rightarrow A_6\} \wedge \\
 &\{(x \geq 0 \wedge y > 0 \wedge q' = q + 1 \wedge x' = (q + 1)y + r) \Rightarrow A_7\}
 \end{aligned}$$

(b)

$$S_1 : q = 0$$

$$S_2 : r = x$$

$$S_3 : \text{while } (r \geq y) \{$$

$$S_4 : \quad r = r - y$$

$$S_5 : \quad q = q + 1$$

}

- 1) $\{x \geq 0 \wedge y \geq 0\} S_1 \{x \geq 0 \wedge y \geq 0 \wedge q = 0\}$ Assignment rule
- 2) $\{x \geq 0 \wedge y \geq 0 \wedge q = 0\} S_2 \{x \geq 0 \wedge y \geq 0 \wedge q = 0 \wedge r = x\}$ -,-
- 3) $\{x \geq 0 \wedge y \geq 0\} S_1 S_2 \{x \geq 0 \wedge y \geq 0 \wedge q = 0 \wedge r = x\}$ Sequencing
- 4) $\{x = qy + r \wedge r \geq y\} S_4 S_5 \{x = qy + r\}$ While ①, ②
- 5) $\{x = qy + r\} S_3 \{x = qy + r \wedge r < y\}$
- 6) $\{x \geq 0 \wedge y \geq 0 \wedge q = 0 \wedge r = x\} \Rightarrow \{x = qy + r \wedge r \geq y\}$ logical
- 7) $\{x \geq 0 \wedge y \geq 0\} S_1 S_2 S_3 \{x = qy + r \wedge r < y\}$ Sequencing ③, ④ Axiom
- 8) $\{x = qy + r \wedge r < y\} \Rightarrow \{x = qy + r \wedge 0 \leq r < y\}$
- 9) $\{x \geq 0 \wedge y \geq 0\} S_1 S_2 S_3 \{x = qy + r \wedge 0 \leq r < y\}$ Weakening ⑦, ⑧

②

1) Weakest precondition for the given program is : $x \leq 10$

2) $\text{WP}(\text{do } S \text{ while } (b)) = \text{WP}(S; \text{while}(b) \text{ do } S)$
 $= \text{WP}(S, \text{WP}(\text{while}(b) \text{ do } S))$

③

- 1) $\lambda x : \text{Int} \rightarrow T'. \lambda y : \text{Int} ((\lambda z : \text{Int} (x(z+1))) ((\lambda w : \text{Int}. w + 1) y)) : (\text{Int} \rightarrow T') \rightarrow (\text{Int} \rightarrow T')$
- 2) $\emptyset, \{x : \text{Int} \rightarrow T'\} \vdash \lambda y : \text{Int} ((\lambda z : \text{Int}. x(z+1)) ((\lambda w : \text{Int}. w + 1) y)) : (\text{Int} \rightarrow T')$ T-Abs ①
- 3) $\{x : \text{Int} \rightarrow T'\}, y : \text{Int} \vdash ((\lambda z : \text{Int} (x(z+1))) ((\lambda w : \text{Int}. w + 1) y)) : T' \rightarrow \text{T-Abs ②}$
- 4) $\{x : \text{Int} \rightarrow T', y : \text{Int}\} \vdash (\lambda z : \text{Int} (x(z+1))) : \text{Int} \rightarrow T' \xrightarrow{\text{③}} \text{T-App}$
- 5) $\{ \quad, \quad \} \vdash ((\lambda w : \text{Int}. w + 1) y) : \text{Int} \xrightarrow{\text{④}} \text{T-Abs}$
- 6) $\{x : \text{Int} \rightarrow T', y : \text{Int}\}, z : \text{Int} \vdash (x(z+1)) : T' \rightarrow \text{T-Abs ⑤}$
- 7) $\{x : \text{Int} \rightarrow T', y : \text{Int}, z : \text{Int}\} \vdash x : \text{Int} \rightarrow T' \xrightarrow{\text{⑥}} \text{T-App}$
- 8) $\{ \quad, \quad \} \vdash (z+1) : \text{Int} \xrightarrow{\text{⑦}} \text{T-Var}$
- 9) $x : \text{Int} \rightarrow T' \in \{x : \text{Int} \rightarrow T', y : \text{Int}, z : \text{Int}\} \rightarrow \text{T-Var}$
- 10) $(z+1) : \text{Int} \Rightarrow z : \text{Int}, z : \text{Int} \in \{x : \text{Int} \rightarrow T', y : \text{Int}, z : \text{Int}\} \xrightarrow{\text{⑨}} \text{T-Var}$
- 11) $\{x : \text{Int} \rightarrow T', y : \text{Int}\} \vdash (\lambda w : \text{Int}. w + 1) : \text{Int} \rightarrow \text{Int} \xrightarrow{\text{⑩}} \text{T-App}$
- 12) $\{ \quad, \quad \} \vdash y : \text{Int} \xrightarrow{\text{⑪}} \text{T-Abs}$
- 13) $\{x : \text{Int} \rightarrow T', y : \text{Int}\}, w : \text{Int} \vdash (w + 1) : \text{Int} \rightarrow \text{Int} \xrightarrow{\text{⑫}} \text{T-Abs}$
- 14) $w : \text{Int} \in \{x : \text{Int} \rightarrow T', y : \text{Int}, w : \text{Int}\} \xrightarrow{\text{⑬}} \text{T-Var}$
- 15) $y : \text{Int} \in \{x : \text{Int} \rightarrow T', y : \text{Int}, w : \text{Int}\} \xrightarrow{\text{⑭}} \text{T-Var}$

Proof Tree

2)

ID No.	Parent	Environment	Term	Return
0	-	\emptyset	$\lambda x: (\text{Int} \rightarrow T'). \lambda y: \text{Int}. (\lambda z: \text{Int} (x(z+1))) ((\lambda w: \text{Int}. w+1) y)$	$(\text{Int} \rightarrow T')$ → $(\text{Int} \rightarrow T')$
1	0	$\{x: \text{Int} \rightarrow T'\}$	$\lambda y: \text{Int} (\lambda z: \text{Int} (x(z+1))) ((\lambda w: \text{Int}. w+1) y)$	$\text{Int} \rightarrow T'$
2	1	$\{x: \text{Int} \rightarrow T', y: \text{Int}\} \rightarrow T_1$	$(\lambda z: \text{Int} (x(z+1))) ((\lambda w: \text{Int}. w+1) y)$	T'
3	2	$\{x: \text{Int} \rightarrow T', y: \text{Int}\}$	$(\lambda z: \text{Int} (x(z+1)))$	$\text{Int} \rightarrow T'$
5	3	$\{y: \text{Int}, x: \text{Int} \rightarrow T', z: \text{Int}\} \rightarrow T_2$	$(x(z+1))$	T'
6	5	T_2	x	$\text{Int} \rightarrow T'$
7	5	T_2	$z+1$	Int
4	2	T_1	$((\lambda w: \text{Int}. w+1) y)$	Int
10	4	T_1	$(\lambda w: \text{Int}. w+1)$	$\text{Int} \rightarrow \text{Int}$
12	10	$\{x: \text{Int} \rightarrow T', y: \text{Int}, w: \text{Int}\}$	$w+1$	Int
11	4	T_1	y	Int