

Ex 34

$$3) \{a \geq 0 \wedge b \geq 0\} \leq \{a = bq + r \wedge a \geq 0 \wedge r < b\}$$

$S = \left(\begin{array}{l} q := 0; \\ r := a; \\ \text{while } b \leq r \text{ do} \\ \quad \left(\begin{array}{l} q := q + 1; \\ r := r - b; \end{array} \right) \\ \text{done} \end{array} \right) S_{\text{init}}$

• Invariant:

The program is computing the euclidean division of a by b .
+ The first precondition is already in the shape of $I \wedge \rightarrow \text{cond}^*$
 $\Rightarrow I = a = bq + r \wedge a \geq 0$
* maybe not always the case!

• General form of the proof

Step 1: we show that $\{a \geq 0 \wedge b \geq 0\} S_{\text{init}} \{I\}$

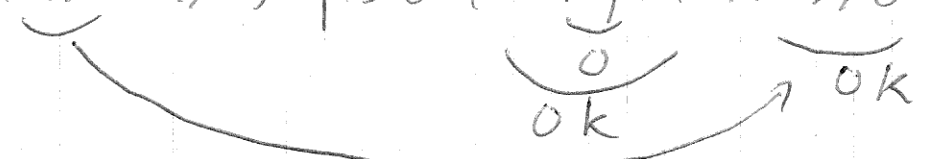
Step 2: we show that $\{I\} \text{while } b \leq r \text{ do } S_{\text{while}} \text{done } \{I \wedge r < b\}$

• Step 1

We apply the rule for composition:

$$T_1 = \frac{\{a \geq 0 \wedge b \geq 0\} q := 0 \{??\} \{??\} r := a \{I\}}{\{a \geq 0 \wedge b \geq 0\} S_{\text{init}} \{I\}}$$

- $\{??\} r := a \{I\}$: $I[a/r] = \{a = bq + r \wedge a \geq 0\}$
 $\Rightarrow ? = \{a = bq + r \wedge a \geq 0\}$

- $\{a \geq 0 \wedge b \geq 0\} q := 0 \{a = bq + r \wedge a \geq 0\}$


Conclusion: $? = \{a = bq + r \wedge a \geq 0\}$

• Step 2

We apply the rules for while and composition:

$$\begin{aligned}
 T_2 = & \frac{\frac{\{I \wedge b \leq n\} q := q + 1 \{?\} \quad \{?\} n := n - b \{I\}}{\{I \wedge b \leq n\} S_{\text{while}} \{I\}}}{\{I\} \text{ while } b \leq n \text{ do } S_{\text{while}} \text{ done } \{I \wedge n < b\}} \\
 & - \{?\} n := n - b \{I\}: \{I\} [n - b / n] \\
 & \quad = \{a = bq + n - b \wedge n - b \geq 0\} \\
 & \quad \Rightarrow ? = \{a = bq + n - b \wedge n - b \geq 0\} \\
 & - \{I \wedge b \leq n\} q := q + 1 \{?\}: \{?\} [q + 1 / q] \\
 & \quad = \{a = b(q + 1) + n - b \wedge n - b \geq 0\} \\
 & \quad = \{a = bq + b + n - b \wedge n - b \geq 0\} \\
 & \text{and } \{I \wedge b \leq n\} \Rightarrow \{a = bq + n \wedge n - b \geq 0\} \text{ since } (n \geq 0 \Rightarrow n - b \geq 0) \\
 & \quad \Rightarrow \text{OK! } ? = \{a = bq + n - b \wedge n - b \geq 0\}
 \end{aligned}$$

Final Tree:

$$\frac{T_1 \quad T_2}{a \geq 0; b \geq 0 \wedge \{a = bq + n \wedge n \geq 0 \wedge n < b\} \text{ [composition]}}$$

Note: The final tree is the proof, everything else is just the reasoning behind building the tree.