Ex 34

3) $\{a \geq 0 \land b \geq 0\}\ S\ \{a = bq + r \land r \geq 0 \land r < b\}$

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

- **Invariant**:

The program is computing the euclidian division of a by b.
+ The final postcondition is already in the shape of $I \land \neg \text{cond}$ *

$\Rightarrow I = a = bq + r \land r \geq 0$

* maybe not always the case!

- General form of the proof

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

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

- Step 1

We apply the rule for composition:

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

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

$\Rightarrow ? = \{a = bq + a \land a \geq 0\}$

- $\{\underbrace{a \geq 0}_{} \land b \geq 0\}\ q := 0\ \{a = \underbrace{\underbrace{bq}_{0}}_{Ok} + a \land \underbrace{a \geq 0}_{Ok}\}$

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

• Step 2

We apply the rules for while and composition:

$$T_2 = \dfrac{\dfrac{\{I \land b \leq r\}\ q := q+1\ \{?\} \qquad \{?\}\ r := r-b\ \{I\}}{\{I \land b \leq r\}\ S_{while}\ \{I\}}}{\{I\}\ \text{while } b \leq r \text{ do } S_{while} \text{ done } \{I \land r < b\}}$$

- $\{?\}\ r := r-b\ \{I\}$: $\{I\}[r-b/r]$

$$= \{a = bq + r - b \land r - b \geq 0\}$$

$$\Rightarrow\ ? = \{a = bq + r - b \land r - b \geq 0\}$$

- $\{I \land b \leq r\}\ q := q+1\ \{?\}$: $\{?\}[q+1/q]$

$$= \{a = b(q+1) + r - b \land r - b \geq 0\}$$

$$= \{a = bq + \cancel{b} + r - \cancel{b} \land r - b \geq 0\}$$

and $\{I \land b \leq r\} \Rightarrow \{a = bq + r \land r - b \geq 0\}$ since $\begin{pmatrix} r \geq 0 \\ b \leq r \end{pmatrix} \Rightarrow r - b \geq 0$

$\Leftrightarrow$ OK! $? = \{a = bq + r - b \land r - b \geq 0\}$

Full tree:

$$\dfrac{T_1 \qquad\qquad T_2}{\{a \geq 0; b \geq 0\}\ S\ \{a = bq + r \land r \geq 0 \land r < b\}}\ \text{(composition)}$$

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