Partial Correctness Proof of Division by Repeated Subtraction

Program

	P: $\{x \geq 0 \;\&\; y > 0\}$	Precondition
S_1	q := 0;	
S_2	r := x;	
	I: $\{x = q \times y + r \;\&\; r \geq 0\}$	Loop Invariant
S_3	while $(r \geq y)$ loop	
	r := r − y;	
	q := q + 1;	
	end loop;	
	Q: $\{x = q \times y + r \;\&\; \neg(r \geq y)\}$	Postcondition

Proof

To prove the above program correct, we divide it into two parts at the loop invariant assertion, and then prove each part in turn. This follows from the Composition rule.

$$\frac{\{P\}S_1; S_2\{I\}, \{I\}S_3\{Q\}}{\{P\}S_1; S_2; S_3\{Q\}} \tag{1}$$

1. $\{x \geq 0 \;\&\; y > 0\}$ q := 0; r := x; $\{x = q \times y + r \;\&\; r \geq 0\}$

   We next use the Composition rule.

$$\frac{\{x \geq 0 \;\&\; y > 0\}q := 0\{P_2\}, \{P_2\}r := x\{x = q \times y + r \;\&\; r \geq 0\}}{\{x \geq 0 \;\&\; y > 0\}q := 0; r := x; \{x = q \times y + r \;\&\; r \geq 0\}} \tag{2}$$

   To derive P_2, we use the axiom of Assignment on the statement r := x.

$$\{x = q \times y + x \;\&\; x \geq 0\}r := x\{x = q \times y + r \;\&\; r \geq 0\} \tag{3}$$

   Therefore, $P_2 \equiv x = q \times y + x \;\&\; x \geq 0$.

   We now have to prove $\{x \geq 0 \;\&\; y > 0\}q := 0\{x = q \times y + x \;\&\; x \geq 0\}$. First we apply the Assignment axiom to derive the weakest precondition for the assignment, which we call P_1.

$$\{x = 0 \times y + x \;\&\; x \geq 0\}q := 0\{x = q \times y + x \;\&\; x \geq 0\} \tag{4}$$

   Therefore, $P_1 \equiv x = 0 \times y + x \;\&\; x \geq 0 \equiv x = x \;\&\; x \geq 0 \equiv x \geq 0$.

   We next apply the Consequence-2 rule to complete this part of the proof.

$$\frac{x \geq 0 \;\&\; y > 0 \Rightarrow P_1, \{P_1\}q := 0\{x = q \times y + x \;\&\; x \geq 0\}}{\{x \geq 0 \;\&\; y > 0\}q := 0\{x = q \times y + x \;\&\; x \geq 0\}} \tag{5}$$

2. $\{x = q \times y + r \;\&\; r \geq 0\}$

   while $(r \geq y)$ loop

   $\quad r := r - y;$

   $\quad q := q + 1;$

   end loop;

   $\{x = q \times y + r \;\&\; \neg(r \geq y)\}$

   To apply the Loop rule, we need the postcondition to be in the form $I \;\&\; \neg(r \geq y) \equiv x = q \times y + r \;\&\; r \geq 0 \;\&\; \neg(r \geq y)$. Therefore, we first apply the Consequence-1 rule.

$$\frac{\{I\}S_3\{I \;\&\; \neg(r \geq y)\}, I \;\&\; \neg(r \geq y) \Rightarrow x = q \times y + r \;\&\; \neg(r \geq y)}{\{I\}S_3\{x = q \times y + r \;\&\; \neg(r \geq y)\}} \tag{6}$$

   Now we may apply the Loop rule

$$\frac{\{I \;\&\; r \geq y\}r := r - y; q := q + 1\{I\}}{\{I\}S_3\{I \;\&\; \neg(r \geq y)\}} \tag{7}$$

   followed by the Composition rule.

$$\frac{\{I \;\&\; r \geq y\}r := r - y\{P_3\}, \{P_3\}q := q + 1\{I\}}{\{I \;\&\; r \geq y\}r := r - y; q := q + 1\{I\}} \tag{8}$$

   To determine P_3, we apply the Assignment axiom.

$$\{x = (q + 1) \times y + r \;\&\; r \geq 0\}q := q + 1\{x = q \times y + r \;\&\; r \geq 0\} \tag{9}$$

   Therefore, $P_3 \equiv x = (q + 1) \times y + r \;\&\; r \geq 0$.

   We apply the Assignment axiom again to prove

$$\{x = (q + 1) \times y + (r - y) \;\&\; (r - y) \geq 0\}r := r - y\{x = (q + 1) \times y + r \;\&\; r \geq 0\} \tag{10}$$

   Note that $x = (q + 1) \times y + (r - y) \;\&\; (r - y) \geq 0 \equiv x = q \times y + y + r - y \;\&\; r \geq y \equiv x = q \times y + r \;\&\; r \geq y$.

   Applying the Consequence-2 rule completes the proof.

$$\frac{I \;\&\; r \geq y \Rightarrow x = q \times y + r \;\&\; r \geq y, \{x = q \times y + r \;\&\; r \geq y\}r := r - y\{x = (q + 1) \times y + r \;\&\; r \geq 0\}}{\{I \;\&\; r \geq y\}r := r - y\{x = (q + 1) \times y + r \;\&\; r \geq 0\}} \tag{11}$$

Thus the partial correctness proof of the given program consists of steps 1-11.