

Consider the following IMP program, which computes y to be the factorial of x :

$$w = (\text{while } 1 \leq x \text{ do } (y := x * y; x := x - 1))$$

We wish to prove the partial-correctness of program w . That is, we wish to prove the following partial-correctness assertion:

$$\{(x = \bar{n}) \wedge (\bar{n} \geq 0) \wedge (y = 1)\} w \{y = \bar{n}!\}$$

The first step is to find a suitable loop invariant I for the while-loop. Suitable loop invariants always satisfy two criteria:

1. I must be valid every time the loop condition is evaluated.
2. I conjoined with the *negation* of the loop condition must imply the postcondition.

Both of these two criteria must be satisfied to prove correctness. If you choose an invariant that is too weak, it will not be strong enough to prove the postcondition and condition 2 will fail. If you choose one that is too strong, it will be falsified on some loop iterations and condition 1 will fail.

For example, suppose we choose $y = \bar{n}!$ as our invariant. This is clearly strong enough to prove the postcondition (since it is identical to the postcondition) but it is not valid on every iteration. Instead, we might try $y(x!) = \bar{n}!$. This is valid on every iteration but it is not quite strong enough to prove the postcondition. To prove the postcondition we would also need to know that $x = 0$ at the end of the loop. The negation of the loop condition is $x < 1$, so to infer that $x = 0$ we need only combine this with $x \geq 0$. This leads us to the invariant $I \equiv (x \geq 0) \wedge (y(x!) = \bar{n}!)$, which is valid on every iteration and, when conjoined with the negation of the loop condition, implies the postcondition.

Armed with this invariant, we can begin our proof as follows:

$$\frac{\frac{\mathcal{D}}{\frac{\{I \wedge (1 \leq x)\} y := x * y; x := x - 1 \{I\}}{\{I\} w \{\neg(1 \leq x) \wedge I\}} \quad (5)}{\vdash A_1} \quad \frac{\quad}{\vdash A_2} \quad (6)}{\{(x = \bar{n}) \wedge (\bar{n} = 0) \wedge (y = 1)\} w \{y = \bar{n}!\}}$$

where assertions A_1 and A_2 are defined by

$$\begin{aligned} A_1 &\equiv (x = \bar{n}) \wedge (\bar{n} \geq 0) \wedge (y = 1) \implies I \\ A_2 &\equiv \neg(1 \leq x) \wedge I \implies (y = \bar{n}!) \end{aligned}$$

(You should convince yourself that assertions A_1 and A_2 are both tautological before continuing.)

Next we must fill in derivation \mathcal{D} . Rule 2 says that to prove a partial-correctness assertion involving a sequence of commands, we must find an assertion C that can serve as a postcondition for the first command and a precondition for the second. So we want a derivation of the form:

$$\mathcal{D} = \frac{\frac{\mathcal{D}_1}{\{I \wedge (1 \leq x)\}y:=x * y\{C\}} \quad \frac{\mathcal{D}_2}{\{C\}x:=x-1\{I\}}}{\{I \wedge (1 \leq x)\}y:=x * y; x:=x-1\{I\}} \quad (2)$$

for some assertion C . If we use Rule 4 to complete sub-derivation \mathcal{D}_2 , then C must be

$$C \equiv I[x-1/x] \equiv (x-1 \geq 0) \wedge (y(x-1)! = \bar{n}!)$$

To complete the proof, we only need to finish derivation \mathcal{D}_1 for our chosen C . Rule 4 says that if the postcondition is C then the precondition must be $C' \equiv C[xy/y] \equiv (x-1 \geq 0) \wedge (xy(x-1)! = \bar{n}!)$. Completing the proof therefore requires using the rule of consequence to show that $I \wedge (1 \leq x)$ implies C' :

$$\mathcal{D}_1 = \frac{\models A_3 \quad \frac{\overline{\{C'\}y:=x * y\{C\}}^{(4)}}{\{I \wedge (1 \leq x)\}y:=x * y\{C\}} \quad \models C \Rightarrow C}{\{I \wedge (1 \leq x)\}y:=x * y\{C\}} \quad (6)$$

where assertion A_3 is given by

$$A_3 \equiv I \wedge (1 \leq x) \Longrightarrow C'$$

(Once again, you should convince yourself that this assertion is really valid.)

The final proof therefore looks like this:

$$\frac{\frac{\models A_3 \quad \frac{\overline{\{C'\}y:=x * y\{C\}}^{(4)}}{\{I \wedge (1 \leq x)\}y:=x * y\{C\}} \quad \models C \Rightarrow C}{\{I \wedge (1 \leq x)\}y:=x * y\{C\}} \quad (6) \quad \frac{\overline{\{C\}x:=x-1\{I\}}^{(4)}}{\{C\}x:=x-1\{I\}} \quad (2)}{\frac{\{I \wedge (1 \leq x)\}y:=x * y; x:=x-1\{I\}}{\{I\}w\{\neg(1 \leq x) \wedge I\}} \quad (5)} \quad (6)}{\frac{\models A_1 \quad \frac{\overline{\{I\}w\{\neg(1 \leq x) \wedge I\}}}{\{(x = \bar{n}) \wedge (\bar{n} \geq 0) \wedge (y = 1)\}w\{y = \bar{n}!\}} \quad (6)}{\{(x = \bar{n}) \wedge (\bar{n} \geq 0) \wedge (y = 1)\}w\{y = \bar{n}!\}} \quad (6)}{\{(x = \bar{n}) \wedge (\bar{n} \geq 0) \wedge (y = 1)\}w\{y = \bar{n}!\}} \quad (6)} \quad (6)$$

where assertions I , C , C' , A_1 , A_2 , and A_3 are defined by:

$$\begin{aligned} I &\equiv (x \geq 0) \wedge (yx! = \bar{n}!) \\ C &\equiv (x-1 \geq 0) \wedge (y(x-1)! = \bar{n}!) \\ C' &\equiv (x-1 \geq 0) \wedge (xy(x-1)! = \bar{n}!) \\ A_1 &\equiv (x = \bar{n}) \wedge (\bar{n} \geq 0) \wedge (y = 1) \Longrightarrow I \\ A_2 &\equiv \neg(1 \leq x) \wedge I \Longrightarrow (y = \bar{n}!) \\ A_3 &\equiv I \wedge (1 \leq x) \Longrightarrow C' \end{aligned}$$