Sample solution to exercise 3, problem 1.15: Preconditions and postconditions

A complete precondition is sought for the given postcondition P:

$$gl<gr\leq ig \text{ and}_{i=gl+1}^{gr}\ x(i)=x(gr) \text{ and}_{i=gr+1}^{ig}\ x(gr)<x(i)$$

with respect to the program segment x(gl):=:x(gr); gr:=gr-1; gl:=gl-1. By proof rules S1 and A1,

$$[[P^{gl}_{gl-1}]^{gr}_{gr-1}]^{x(gl),x(gr)}_{x(gr),x(gl)}$$

is such a complete precondition.

$$[P^{gl}_{gl-1}]^{gr}_{gr-1}$$

=

$$gl<gr\leq ig+1 \text{ and}_{i=gl}^{gr-1}\ x(i)=x(gr-1) \text{ and}_{i=gr}^{ig}\ x(gr-1)<x(i)$$

In this expression every reference to x(gl) must be replaced by x(gr) and, simultaneously, every reference to x(gr) must be replaced by x(gl). The references to x(gr-1) are problematic because gr-1 may — but need not — be equal to gl. The first term in the first and series (which is not empty) states that x(gl)=x(gr-1). By using this fact one can eliminate the references to x(gr-1). We rewrite the above expression accordingly:

=

$$gl<gr\leq ig+1 \text{ and } x(gl)=x(gr-1) \text{ and}_{i=gl}^{gr-1}\ x(i)=x(gr-1) \text{ and}_{i=gr}^{ig}\ x(gr-1)<x(i)$$

=

$$gl<gr\leq ig+1 \text{ and } x(gl)=x(gr-1) \text{ and}_{i=gl}^{gr-1}\ x(i)=x(gl) \text{ and}_{i=gr}^{ig}\ x(gl)<x(i)$$

= [x(gl)=x(gr-1) is equivalent to the last term in the first (non-empty) and series.]

$$gl<gr\leq ig+1 \text{ and}_{i=gl}^{gr-1}\ x(i)=x(gl) \text{ and}_{i=gr}^{ig}\ x(gl)<x(i)$$

= [The first term in the first (non-empty) series is a tautology.]

$$gl<gr\leq ig+1 \text{ and}_{i=gl+1}^{gr-1}\ x(i)=x(gl) \text{ and}_{i=gr}^{ig}\ x(gl)<x(i)$$

The first reference to x(.) in this expression is never to be replaced, because i≠gl and i≠gr. The second and third references to x(.) (to x(gl)) must always be replaced. The last reference to x(i) is to be replaced only in the first term of that and series; therefore that term must be taken out of the series. This series can, however, be empty. We therefore rewrite the last expression above as follows:

=

$$gl<gr\leq ig+1 \text{ and}_{i=gl+1}^{gr-1}\ x(i)=x(gl)$$
$$\text{and } [gr>ig \text{ or } gr\leq ig] \text{ and}_{i=gr}^{ig}\ x(gl)<x(i)$$

=

$gl<gr\leq ig+1 \text{ and}_{i=gl+1}^{gr-1} x(i)=x(gl)$

$\text{and } [gr>ig \text{ or } gr\leq ig \text{ and}_{i=gr}^{ig} x(gl)<x(i)]$

=

$gl<gr\leq ig+1 \text{ and}_{i=gl+1}^{gr-1} x(i)=x(gl)$

$\text{and } [gr>ig \text{ or } gr\leq ig \text{ and } x(gl)<x(gr) \text{ and}_{i=gr+1}^{ig} x(gl)<x(i)]$

$[=[P^{gl}_{gl-1}]^{gr}_{gr-1}]$

The references to x(i) in the last expression above are never to be replaced, because either $gl<i<gr$ or $gl<gr<i$, which imply that $i\neq gl$ and $i\neq gr$ in both situations. Each other reference to x(.) is a reference to x(gl) or to x(gr) and must therefore always be replaced.

The complete precondition sought is, therefore,

$[[P^{gl}_{gl-1}]^{gr}_{gr-1}]^{x(gl),x(gr)}_{x(gr),x(gl)}$

=

$gl<gr\leq ig+1 \text{ and}_{i=gl+1}^{gr-1} x(i)=x(gr)$

$\text{and } [gr>ig \text{ or } gr\leq ig \text{ and } x(gr)<x(gl) \text{ and}_{i=gr+1}^{ig} x(gr)<x(i)]$

= [an empty and series is true]

$gl<gr\leq ig+1 \text{ and}_{i=gl+1}^{gr-1} x(i)=x(gr)$

$\text{and } [gr>ig \text{ or } gr\leq ig \text{ and } x(gr)<x(gl)] \text{ and}_{i=gr+1}^{ig} x(gr)<x(i)$

= [x(gr)=x(gr) is a tautology]

$gl<gr\leq ig+1 \text{ and}_{i=gl+1}^{gr} x(i)=x(gr)$

$\text{and } [gr>ig \text{ or } x(gr)<x(gl)] \text{ and}_{i=gr+1}^{ig} x(gr)<x(i)$

Depending upon the use to which the expression will be subsequently put, either of the above three expressions could be the most suitable one. Any of these is an acceptable solution to the problem as stated.

(end)