Sometimes auxiliary variables are necessary

The following is a well-known proof of $\{x=0\}\ (x:=x+1 \ \| \ x:=x+1)\ \{x=2\}$. This proof involves auxiliary variables (also called "ghost variables") a and b :

precondition : $x=0 \wedge a=0 \wedge b=0$
global invariant: $x=a+b$

$$
\begin{array}{lllll}
(& \{a=0\} & x,a := x+1,a+1 & \{a=1\} \\
\| & \{b=0\} & x,b := x+1,b+1 & \{b=1\} \\
) & & &
\end{array}
$$

The correctness of this annotation is easily verified and $x=a+b \wedge a=1 \wedge b=1$ implies the post-condition $x=2$.

Suppose we deny ourselves the use of auxiliary variables, then what is the best we can prove about the program $x:=x+1 \ \| \ x:=x+1$? More precisely, what is the strongest postcondition R for which assertions P0, Q0, P1, Q1 exist such that the following annotation is correct ?

$$
\begin{array}{llll}
\{x=0\} & & & \\
(& \{P0\} & x:=x+1 & \{Q0\} \\
\| & \{P1\} & x:=x+1 & \{Q1\} \\
) & & & \\
\{R\} . & & &
\end{array}
$$

First, we observe that in the above annotation both $P0$ and $P1$ may be strengthened to $P0 \wedge P1$ and, similarly, $Q0$ and $Q1$ may be strengthened to $Q0 \wedge Q1$, without violating the correctness of the annotation. As a result, we may (and will) confine our attention to symmetric annotations of the following form:

$$
\begin{array}{l}
\{ x = 0 \} \\
(\ \{P\} \ x := x+1 \ \{Q\} \\
\| \ \{P\} \ x := x+1 \ \{Q\} \\
) \\
\{R\} \ .
\end{array}
$$

The proof obligations for this annotation are:

(0)	$[x=0 \Rightarrow P]$	(local correctness of P)
(1)	$[P \Rightarrow Q(x:=x+1)]$	(local correctness of Q)
(2)	$[P \Rightarrow P(x:=x+1)]$	(global correctness of P)
(3)	$[P \wedge Q \Rightarrow Q(x:=x+1)]$	(global correctness of Q)
(4)	$[Q \Rightarrow R]$	(correctness of R)

The strongest R satisfying (4) is of course Q. Proof obligation (3) is absorbed by (1) and the strongest Q satisfying (1) is $P(x:=x-1)$, because $x:=x-1$ and $x:=x+1$ are each other's inverses. Finally, by mathematical induction, $(0) \wedge (2)$ is equivalent to

(5) $\quad [x \geq 0 \Rightarrow P]$,

whose strongest solution is of course $[P \equiv x \geq 0]$. Thus, the following annotation is the best possible for (given) precondition $x=0$:

$\{x=0\}$
$(\ \{x\geq 0\}\ x:=x+1\ \{x\geq 1\}$
$\|\ \{x\geq 0\}\ x:=x+1\ \{x\geq 1\}$
$)$
$\{x\geq 1\}$.

The above shows that we sometimes really need auxiliary variables to prove what we want to prove about our programs .

Eindhoven, 10 january 1993
Rob R. Hoogerwoord
department of mathematics and computing science
Eindhoven University of Technology