On an argument by J.A. Carruth & J. Misra

In [0], Carruth & Misra start the analysis of the last case with

"• Executing γ_i, $i \neq k$: We show that $\neg d_k$ is a precondition for the execution of γ_i. Since the effective execution of γ_i preserves $\neg d_k$, we have then $\neg d_k \vee x = k$ as a postcondition.

We prove that $\neg d_k$ is a precondition by assuming d_k as a precondition and deriving a contradiction."

* * *

The first purpose of this note is to show that, had the authors stuck to the standard proof format for the proof obligations, they would never have come up with (so many rabbits and) a reductio ad absurdum.

Its second purpose is to polish – if not to correct – their use of the Axiom of Assignment.

* * *

The purpose of the proof part under consideration is to show that the precondition of γ_i for $i \neq k$ is at least as strong as

$$wp.\gamma_i.(\neg d_k \vee x = k) \quad .$$

To this end we may use

- the properties of "now", in particular

(0) $\bar{p} \leq$ now (for all variables $\bar{p}$ of the appropriate type).

- the "timing constraints"

(1) $c_i \Rightarrow \bar{c}_i \leq 1 + \bar{b}_i$
(2) $d_i \Rightarrow \bar{c}_i \leq 1 + \bar{b}_i$
(3) $d_i \Rightarrow 1 + \bar{c}_i < \bar{d}_i$

for all i in the range concerned

- the "invariants"

(4) $x = k \Rightarrow \bar{b}_i \leq \bar{c}_k$
(5) $d_k \Rightarrow x = k$

for all i, k in the range concerned

- the definition of γ_i:

(6) $\{\gamma_i\}\ s_i, x, \bar{c}_i := c, i, \text{now}$ if $s_i = b$.

As we shall see shortly, x quickly disappears from our proof obligation; in anticipation we "eliminate" x from our givens by using (4) and (5) to conclude

(7) $d_k \Rightarrow \bar{b}_i \leq \bar{c}_k$.

We now proceed by observing for $i \neq k$:

$$\begin{aligned} & wp.\gamma_i.(\neg d_k \vee x = k) \\ = & \quad \{(6)\} \\ & wp.(s_i, x, \bar{c}_i := c, i, \text{now}).(\neg d_k \vee x = k) \\ = & \quad \{\text{Axiom of Assignment}\} \end{aligned}$$

$$
\begin{array}{ll}
 & \neg d_k \ \vee \ i = k \\
= & \quad \{ \ i \neq k \} \\
 & \neg d_k \\
\Leftarrow & \quad \{ \ (7); \ (3) \text{ with } i := k \} \\
 & \bar{b}_i > \bar{c}_k \quad \vee \quad 1 + \bar{c}_k \geqslant \bar{d}_k \\
\Leftarrow & \quad \{ \text{arithmetic}; \ (0) \text{ with } \bar{p} := \bar{d}_k \} \\
 & 1 + \bar{b}_i > 1 + \bar{c}_k \ \vee \ 1 + \bar{c}_k \geqslant \text{now} \\
\Leftarrow & \quad \{ \text{"transitivity" } \geqslant, > \} \\
 & 1 + \bar{b}_i \geqslant \text{now} \qquad .
\end{array}
$$

In order to establish that the precondition of γ_i implies the latter inequality, the authors argue – here one should know that c_i is short for $s_i = c$ –

" Following the execution of γ_i, timing constraint (T1) holds, i.e.,

(T1) $\qquad (c_i \vee d_i) \Rightarrow \bar{c}_i \leqslant 1 + \bar{b}_i$.

The effective execution of γ_i sets c_i to true and $\bar{c}_i$ to now. Applying the axiom of assignment (to replace c_i by true and $\bar{c}_i$ by now)

[...] $\qquad$ now $\leqslant 1 + \bar{b}_i$

holds prior to the effective execution of γ_i."

(Note that their (T1) is the conjunction of our (1) and (2).)

I would like to point out that from the

fact that P holds after the execution of S we are not allowed to conclude that

$$wp.S.P$$

holds prior to the execution of S! From the fact that P holds after the execution of S, we are only allowed to conclude that the execution of S is guaranteed not to establish $\neg P$; we are allowed to conclude that

$$\neg\, wp.S.(\neg P)$$

holds prior to the execution of S. Failing to distinguish between wp.S and its conjugate $(wp.S)^*$ is a common source of flaws in mixed postulational/operational arguments; A.D. 1992, both authors should have known better than to mix these two types of arguments. Timing constraint (2) is superfluous.

[0] Proof of a Real-Time Mutual-Exclusion Algorithm, Notes on UNITY: 32-92, by John Allen Carruth & Jayadev Misra, Sep. 10, 1992

Austin, 28 April 1994

prof. dr. Edsger W. Dijkstra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712-1188
USA