

Copyright Notice

The following manuscript

EWD 573: A great improvement

is held in copyright by Springer-Verlag New York.

The manuscript was published as pages 217–219 of

Edsger W. Dijkstra, *Selected Writings on Computing: A Personal Perspective*,
Springer-Verlag, 1982. ISBN 0-387-90652-5.

**Reproduced with permission from Springer-Verlag New York.
Any further reproduction is strictly prohibited.**

A great improvement.

After my return from my last trip the first thing W.H.J. Feijen en M. Rem showed me was a much improved definition of "wdec", for which they gave the credit to my colleague F.E.J. Kruseman Aretz. In [1] I had written:

"More specifically: we shall use the notation $wp(S, R)$, where S denotes a statement list and R some condition on the state of the system, to denote the weakest pre-condition for the initial state of the system such that activation of S is guaranteed to lead to a properly terminating activity leaving the system in a final state satisfying the post-condition R ."

For a well-chosen programming language the article continues by defining how for any given S and R the pre-condition $wp(S, R)$ is derived. One page later, when dealing with a repetitive construct and its termination, [1] continues:

"Let t denote some integer function, defined on the state space, and let $wdec(S, t)$ denote the weakest pre-condition such that activation of S is guaranteed to lead to a properly terminating activity leaving the system in a final state such that the value of t is decreased by at least 1 (compared to its initial value). [...] The relation between wp and $wdec$ is as follows. For any point X in state space we can regard $wp(S, t \leq t_0)$ as an equation with t_0 as the unknown. Let its smallest solution for t_0 be $tmin(X)$. (Here we have added the explicit dependence on the state X .) Then $tmin(X)$ can be interpreted as the lowest upper bound for the final value of t if the mechanism S is activated with X as initial state. Then, by definition, $wdec(S, t) = (tmin(X) \leq t(X) - 1) = (tmin(X) < t(X))$."

Kruseman Aretz's definition is

$$wdec(S, t) = wp(S, t < t_0)_t^{t_0}$$

where the notation R_y^x is used to denote a copy of the expression R in which each occurrence of the variable x is replaced by y (or by (y) if necessary).

Example. Let S be
 if true \rightarrow $x := x - y$
 || true \rightarrow $x := x - z$
 fi

and let $t = x$.

Then --see [1]-- we have:

$$\begin{aligned} \text{wp}(S, t < t_0) &= \\ &(\text{true} \text{ or } \text{true}) \text{ and } (\text{true} \Rightarrow \text{wp}("x := x - y", x < t_0)) \\ &\quad \text{and } (\text{true} \Rightarrow \text{wp}("x := x - z", x < t_0)) = \\ &\text{wp}("x := x - y", x < t_0) \text{ and } \text{wp}("x := x - z", x < t_0) = \\ &(x - y < t_0) \text{ and } (x - z < t_0) . \end{aligned}$$

Hence $\text{wdec}(S, t) = \text{wp}(S, t < t_0) \stackrel{t_0}{t} = (x - y < x) \text{ and } (x - z < x) = y > 0 \text{ and } z > 0$

This is much simpler than my original treatment. Analogous to the first five lines, we would have to derive first

$$\text{wp}(S, t \leq t_0) = (x - y \leq t_0) \text{ and } (x - z \leq t_0) .$$

Then we would have to find the smallest solution for t_0 satisfying that equation --and that is not a very standard operation!--; in this case we would find

$$t_{\min} = \max(x - y, x - z)$$

and then we would derive

$$\begin{aligned} \text{wdec}(S, t) &= t_{\min} < t = \max(x - y, x - z) < x = \max(-y, -z) < 0 = \\ &\min(y, z) > 0 . \end{aligned}$$

(End of example.)

The example shows that Kruseman Aretz's alternative definition does not only embody a conceptual simplification, but that it also smooths the formal labour to be performed. It couples in a very direct way the derived condition wdec with the fundamental condition wp in a way that is very familiar from the axiom of assignment.

* * *

In retrospect I blame myself for acquiescing in my ugly original definition. I knew quite well that it was ugly: it was preceded in [1] by "Note (which can be skipped at first reading)." But I have failed to hear my own warning!

* * *

It was only after the above had been typed that I was told about the heuristics that had led to the new formulation of wdec . For that part, Kruseman Aretz gave the credit to M.Rem: it seems to have been the typical multi-person achievement, in which it is very hard to reconstruct later who has contributed what.

The argument is the following. Let us introduce an auxiliary variable, t_0 say, in which the value of t is recorded prior to the execution of S . (For the sake of this recording we assume that the value of t can be "computed", so that it can be assigned to t_0 .) Then we define

$$wdec(S, t) = wp("t_0 := t; S", t < t_0)$$

because the weakest pre-condition that " $t_0 := t; S$ " is guaranteed to establish $t < t_0$ is, indeed, the weakest pre-condition for S such that S is guaranteed to decrease t (by at least one, because t is an integer-valued function). But, thanks to the axiom of concatenation, this right-hand side reduces to

$$= wp(t_0 := t, wp(S, t < t_0))$$

which, thanks to the axiom of assignment, reduces to

$$= wp(S, t < t_0) \frac{t_0}{t}$$

and that is exactly the expression I gave on EWD573 - 0.

- [1] Dijkstra, Edsger W., Guarded Commands, Nondeterminacy and Formal Derivation of Programs. Comm.ACM 18, 8 (Aug. 1975) 453 - 457.

Plataanstraat 5
NL-4565 NUENEN
The Netherlands

prof.dr.Edsger W.Dijkstra
Burroughs Research Fellow