An immediate sequel to EWD398: "Sequencing primitives revisited.".

I have fixed the semantic definition of the if...fi and of the do...od constructs as introduced in EWD398.

Let "Sif" be: if B1:S1 [] ... [] Bn:Sn fi   ; then $wp(Sif, P) =$

$\{(E\ i: 1 \leq i \leq n: Bi)$ and $(A\ i: 1 \leq i \leq n:(Bi$ and $wp(Si, P))$ or non $Bi)\}$.

Let "Sdo" be: do B1:S1 [] ... [] Bn:Sn od   ; then $wp(Sdo, P) =$

$(E\ i: 0 \leq i: H_i(Sdo, P))$, where the $H_i(Sdo, P)$ are given by the recurrence relation: $H_0(Sdo, P) = \{P$ and non $(E\ j: 1 \leq j \leq n: Bi)\}$

for $i > 0$: $H_i(Sdo, P) = \{wp(Sif, H_{i-1}(Sdo, P))$ or $H_{i-1}(Sdo, P)\}$.

Here the "$wp(Sif, ...)$ is the function defined above. The interpretation of $H_i(Sdo, P)$ is "the weakest precondition such that we can guarantee termination after at most i executions of a guarded command such that then the postcondition P will be satisfied. It is indeed the weakest precondition, if initially $wp(Sdo, P)$ is not satisfied, either non-termination or termination without establishing the truth of P or both are possible. In terms of the H_i an alternative definition of the weakest precondition for the do...od construct could have been --but I prefer to avoid the limit concept--

$$wp(Sdo, P) = \lim_{i \to inf} H_i(Sdo, P)$$

so we had better forget this again.

The decision to postulate --EWD398 - 4, last paragraph-- "fair random selection" so that the construct as described on top of page 5 and in the middle of page 8 is guaranteed to terminate, was a mistake: for such constructs we prefer now not to exclude non-termination. It is just too tricky if the termination --and in particular: the proof of the termination-- has to rely on the fair randomness of the selection and we had better restrict ourselves to constructs were each guarded command, when executed, implies a further approaching of the terminal state.

27th November 1973   prof.dr.Edsger W.Dijkstra

Burroughs   Research Fellow

Plataanstraat 5

NUENEN - 4565, The Netherlands