A note on substitution and renaming

The formal definition of the semantics of the assignment statement $x := E$ uses the predicate denoted by

$$P^x_E \qquad \text{or} \qquad P[E/x] \qquad ;$$

it is the predicate derived from P by "replacing each occurrence of x in P by E". In the context of the assignment statement the derived predicate is to be understood in the same state space as P; in other words, in general, x occurs in E. In the latter case, the substitution is a complicated operation in the sense that it both eliminates and reintroduces x.

Some time ago I wanted to separate those two aspects by restricting the substitution to substituting the fresh variable x' for x. In that case, we have two alternative expressions for P^x_E:

$$(0) \qquad (\underline{E}x' :: x' = E \wedge P^x_{x'})$$

$$(1) \qquad (\underline{A}x' :: x' \neq E \vee P^x_{x'}) \quad ,$$

the two expressions being equivalent because —see EWD 834— $(\underline{N}x' :: x' = E) = 1$. Formulation (1) has some preference because we normally deal with predicate transformers that distribute over conjunctions.

In the language fragment of "A Discipline of Programming", I avoided conditional expressions because, in my case, they would introduce "nondeterministic expressions" and I was not able to substitute them for a variable. Formulation (1), however, shows us the way how to do it.

The semantics of the above assignment statement

$x := E$ is equally well captured by the predicate

(2) $$x' = E$$

(Note that, since, in general, x occurs in E, this is a predicate on the Cartesian product of initial and final state space — the latter one being the primed one — .) Denoting (2) by Q, (1) takes the form

(3) $$(\underline{A}x' :: \neg Q \vee P^x_{x'})$$;

E being a "deterministic expression" is reflected by $(\underline{N}x' :: Q) = 1$.

But this is easily generalized. With the assignment statement $x := E$ we associate the predicate Q — in x and x' — such that the possible values of E are precisely the roots of $x' : Q$ (i.e. of Q, when viewed as an equation in x').

Example With $\underline{\text{if}}$ true $\to +1$ ▯ true $\to -1$ $\underline{\text{fi}}$ for E, we find $x' = 1 \vee x' = -1$ (or $abs(x') = 1$) for Q. (End of Example.)

With the above Q, wp("$x := E$", P) is again given by (3). In other words, once we have decided to restrict substitution to "priming" or "renaming", "nondeterministic expressions" are in a limited sense given for free —limited only because (3) might be harder to manipulate— .

Newcastle-upon-Tyne

Plataanstraat 5
5671 AL NUENEN
The Netherlands

7 September 1982

prof. dr. Edsger W. Dijkstra
Burroughs Research Fellow