On subgoal induction.

In [1] I encountered "subgoal induction" as a technique for proving partial correctness. It was applied to a program S that I would write down as

$$
\begin{aligned}
S:\quad & x := f(x0);\\
& \underline{\text{do}}\ B(x) \rightarrow x := g(x)\ \underline{\text{od}};\\
& x := h(x)\quad .
\end{aligned}
$$

In order to prove

$$\{P(x0)\}\ \ S\ \ \{R(x0,\ x)\} \tag{1}$$

--i.e. if $P(x0)$ holds and the execution of S terminates properly, then in the final state $R(x0, x)$ will hold-- "subgoal induction" is used. The technique consists of finding a relation $Q(x, z)$ satisfying

$$(\underline{A}\ x:\ (\underline{\text{non}}\ B(x)) \Rightarrow Q(x,\ h(x))) \tag{2}$$

$$(\underline{A}\ x,\ z:\ (Q(g(x),\ z)\ \underline{\text{and}}\ B(x)) \Rightarrow Q(x,\ z)) \tag{3}$$

$$(\underline{A}\ x,\ z:\ (P(x)\ \underline{\text{and}}\ Q(f(x),\ z)) \Rightarrow R(x,\ z)) \tag{4}$$

and it was stated that the existence of a relation Q satisfying (2), (3) and (4) proves (1).

My general inclination when I encounter such formulae --particularly when I encounter them in a report that is really dealing with something else-- is to skim them, assuming that they are no more than variations on an old theme. Formula (3), however, attracted my attention, because, if $P'(x)$ is the invariant relation for the repetitive construct, we have to prove --see [2]--

$$(P'(x)\ \underline{\text{and}}\ B(x)) \Rightarrow P'(g(x)) \tag{5}$$

and, if we compare (5) with (3), we see that the substitution of $g(x)$ for x occurs at the other side of the implication! This was reason enough to investigate subgoal induction a little bit more closely.

In terms of a relation Q satisfying (2), (3), and (4), we can take as our invariant relation

$$P'(x):\quad (\underline{A}\ z:\ Q(x,\ z) \Rightarrow Q(f(x0),\ z)) \tag{6}$$

a relation which is clearly established by "$x := f(x0)$" , the first statement of S . To prove (5) we have to prove

$$((\underline{A}\ z:\ Q(x,\ z) \Rightarrow Q(f(x0),\ z))\ \underline{\text{and}}\ B(x)) \Rightarrow$$

$$((\underline{A}\ z\colon Q(g(x),\ z) \Rightarrow Q(f(x0),\ z)) \tag{7}$$

For those values of x, such that $B(x)$ is false, the implication (7) is vacuously true, for those values of x, such that $B(x)$ is true, (3) tells us that $Q(g(x),\ z)$ is a stronger condition on z than $Q(x,\ z)$, so that whatever is implied by the latter is certainly implied by the former. Hence (7) and thus (5) follows from (3).

Finally we have to prove that

$$(P'(x)\ \underline{\text{and}}\ \underline{\text{non}}\ B(x)) \Rightarrow wp(\text{"}x:= h(x)\text{"},\ R(x0,\ x)) \tag{8}$$

Thanks to (2) and (6), the left-hand side of (8) reduces to

$$(\underline{A}\ z\colon Q(x,\ z) \Rightarrow Q(f(x0),\ z))\ \underline{\text{and}}\ Q(x,\ h(x))$$

from which we conclude --applying the quantified implication for $z = h(x)$-- the truth of

$$Q(f(x0),\ h(x)) \quad .$$

Because the initial value $x0$ satisfies $P(x0)$, we conclude --applying (4) with $x = x0$ and $z = h(x)$-- the truth of

$$R(x0,\ h(x))$$

but thanks to the axiom of assignment this is identical to the right-hand side of (8). Hence (8) frollows from (2), (4), and (6).

Thus we have established that --as was to be expected-- subgoal induction is indeed the next variation on an old theme.

The analysis described above was carried through together with C.S. Scholten.

Plataanstraat 5
NL-4565 NUENEN
The Netherlands

prof.dr.Edsger W.Dijkstra
Burroughs Research Fellow

[1] Is "sometime" sometimes better than "always"? Intermittent assertions in proving program correctness, by Zohar Manna and Richard Waldinger, STAN-CS-76-558

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