Copyright Notice

The following manuscript

EWD 576: On subgoal induction

is held in copyright by Springer-Verlag New York.

The manuscript was published as pages 223–224 of


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

$$S: \quad x := f(x_0);$$
$$\quad \text{do } B(x) \rightarrow x := g(x) \text{ od};$$
$$\quad x := h(x).$$

In order to prove

$$\{p(x_0)\} \; S \; \{r(x_0, x)\} \quad (1)$$

--i.e. if $P(x_0)$ holds and the execution of $S$ terminates properly, then in the final state $R(x_0, x)$ will hold-- "subgoal induction" is used. The technique consists of finding a relation $Q(x, z)$ satisfying

$$(A \; x: (\text{non } B(x)) \Rightarrow Q(x, h(x))) \quad (2)$$
$$\begin{align*}
(A \; x, z: (Q(g(x), z) \text{ and } B(x)) \Rightarrow Q(x, z)) \quad (3) \\
(A \; x, z: (P(x) \text{ and } Q(f(x), z)) \Rightarrow R(x, z)) \quad (4)
\end{align*}$$

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]--

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

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

$${P}'(x): \quad (A \; z: Q(x, z) \Rightarrow Q(f(x_0), z)) \quad (6)$$

a relation which is clearly established by "$x := f(x_0)$", the first statement of $S$. To prove (5) we have to prove

$$((A \; z: Q(x, z) \Rightarrow Q(f(x_0), z)) \text{ and } B(x)) \Rightarrow$$
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

\[
(p(x) \text{ and non } b(x)) \implies wp("x:= h(x)", R(x, 0, x))
\]  

(8)

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

\[
(A z : Q(x, z) \implies Q(f(x0), z)) \text{ and } Q(x, h(x))
\]

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

\[
Q(f(x0), h(x))
\]

Because the initial value \( x0 \) satisfies \( P(x) \), 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) follows 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  prof.dr.Edsger W.Dijkstra
NL-4565 NUENEN  Burroughs Research Fellow
The Netherlands

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