A somewhat open letter to F. Kröger.

Dear Dr. Kröger:

In a recent article [1], you prove - in my notation, see [2] -

$\{a \leq 100 \wedge b = 1\}$
do $100 < a \wedge b \neq 1 \rightarrow a, b := a-10, b-1$
[] $a \leq 100 \rightarrow a, b := a+11, b+1$
od $\{a = 101\}$

Allow me to show you the argument I, as a programmer, came up with.

I rewrote the proof obligation as follows

$\{a \leq 100 \wedge b = 1\}$
do $a \leq 100 \rightarrow a, b := a+11, b+1$ **od**;
$\{P_0$, hence $P_0 \vee P_1 \vee P_2\}$
do $110 < a \wedge b \neq 1 \rightarrow a, b := a-10, b-1$ $\{P_0 \vee P_2\}$
[] $100 < a \leq 110 \wedge b \neq 1 \rightarrow a, b := a-10, b-1$ $\{P_1\}$
[] $a \leq 100 \rightarrow a, b := a+11, b+1$ $\{P_0\}$
od $\{(P_0 \vee P_1 \vee P_2) \wedge 100 < a \wedge b = 1$, hence $a = 101\}$

with $P_0 = 100 < a \leq 111 \wedge b \geq 2$
$P_1 = 90 < a \leq 100 \wedge b \geq 1$
$P_2 = (a = 101) \wedge (b = 1)$.

The two program transformations have no effect. You may <u>always</u> insert before a repet-

itive construct an excerpt from it ; you may always split a guarded command. The first repetitive construct terminates obviously. The verification that $P_0 \vee P_1 \vee P_2$ is an invariant of the second one is simple and straightforward.

In order to prove the termination of the second repetitive construct , we observe
1) the initial truth of P_0. (excluding truth of the last guard)
2) that the truth of P_1 implies the falsity of the first two guards and the truth of the last one.

As a result the last two guarded commands may be merged and the invariant relation may be strengthened. We rewrite the second repetitive construct as follows

$\{P_0$, hence $P_0 \vee P_2\}$
do $110 < a \wedge b \neq 1 \rightarrow a, b := a-10, b-1 \{P_0 \vee P_2\}$
$[\!]$ $100 < a \leq 110 \wedge b \neq 1 \rightarrow a := a+1 \{P_0\}$
od $\{(P_0 \vee P_2) \wedge b = 1$, hence $a = 101\}$

In view of $P_0 \vee P_2$, the first guarded command sets $a = 101$; the second guard remains true until $a = 111$. The guards being mutually exclusive , we may rewrite — note that a loop with only the second guarded command obviously terminates —

$\{P_0 \vee P_2\}$
do $110 < a \wedge b \neq 1 \rightarrow a, b := 101, b-1 \{P_0 \vee P_2\}$
$[]$ $100 < a \leq 110 \wedge b \neq 1 \rightarrow a := 111 \{P_0\}$
od

Because $P_0 \wedge a = 111$ implies the truth of the first guard, by almost the same device as used before, the two guarded commands can be merged, giving

$\{P_0 \vee P_2\}$
do $100 < a \wedge b \neq 1 \rightarrow a, b := 101, b-1 \{P_0 \vee P_2\}$ **od**

which trivially terminates. This concludes a proof with a minimum amount of formal labour.

* * *

When I saw the length of your proof, it put me off; I stopped reading and developed the above argument. I had never really analysed McCarthy's 91-function: it has always struck me as a rather contorted puzzle. After the above proof, I proved the termination, in the style of R.W. Floyd, using a well-founded set; from that I derived a closed formula for the exact number of repetitions. It is neither long, nor difficult; but it is too boring to record here; the steps of the derivation are completely standard.

* * *

In my opinion – but the opinion is a well-considered one – computing science needs the kind of vigorous mathematics that results from a subtle balance between the application of formal techniques and of common sense. (And there are reasons to believe that in computing science that balance is more critical than in many other areas of mathematics.) I trust you can now understand why I find it hard to consider your "Generalized Invariants" of great significance in the context of computing science. Perhaps your paper had better been published in some Journal of Logic than in Acta Informatica, where it gives fuel to the accusation that the latter publishes too much "pompous irrelevance".

[1] Kröger, F.: Infinite Proof Rules for Loops. Acta Informatica 14, 371-389 (1980)

[2] Dijkstra, Edsger W.: A Discipline of Programming. Prentice-Hall, Inc., Englewood Cliffs, N.J., U.S.A.

Plataanstraat 5
5671 AL NUENEN
The Netherlands

11 November 1980
prof.dr. Edsger W. Dijkstra
Burroughs Research Fellow