Some remarks on EWD 372

EINDHOVEN UNIVERSITY OF TECHNOLOGY

Department of Mathematics

Memorandum 1974-04

Issued March, 1974

SOME REMARKS ON EWD 372

by

W. Peremans

University of Technology
Department of Mathematics
PO Box 513, Eindhoven
The Netherlands

Some remarks on EWD 372

by

W. Peremans.

In this note some comments will be given on the so-called "fundamental invariance theorem", contained in the paper "A simple axiomatic basis for programming language constructs" By Edsger W. Dijkstra.

This theorem deals with a recursive procedure H defined by a text built by means of concatenation and binary selection from fixed statements and the variable statement H.
Let H" denote the statement obtained by substituting the statement H' for H in the text of the procedure H and fH" and fH' the corresponding predicate transformers.
The following is stated as the fundamental invariance theorem:
If Q and R are predicates satisfying

$$Q \Rightarrow fH'(R) \text{ implies } Q \Rightarrow fH''(R) ,$$

then

$$Q \text{ and } fH(T) \Rightarrow fH(R) .$$

In the proof the case is treated that the variable H occurs only once in the text of the procedure. This may be translated into the language of transformers in a way similar to EWD 372, p.15 as follows.

In the evaluation of fH"(R) first of all a fixed predicate transformer fS operates on R yielding the argument of the transformer fH'. The transformer mapping fH'(fS(R)) on fH"(R) is called E as in EWD 372. The condition of the theorem may now be enunciated as follows:

(1) for all healthy predicate transformers fH':

$$Q \Rightarrow fH'(R) \text{ implies } Q \Rightarrow E(fH'(fS(R))) .$$

On p.15 of EWD 372 it is stated, that this amounts to (17) of that paper, which in our notation reads

(2) $$R \Rightarrow fS(R) \text{ and } Q \Rightarrow E(Q) .$$

From the monotonicity properties of E and fH' it is clear that (2) implies (1). We investigate whether (1) implies (2). Therefore we suppose (1) satisfied.
We distinguish three cases.

1. $R \Rightarrow fS(R)$ holds and $R \neq F$. Because $R \neq F$, there exists a state q for which R is true. From this and $R \Rightarrow fS(R)$ it follows that there exists a healthy predicate transformer fK, such that $Q = fK(R) = fK(fS(R))$. With (1) we infer $Q \Rightarrow E(fK(fS(R))) = E(Q)$, so (2) is satisfied.

2. $R \Rightarrow fS(R)$ does not hold. In that case there exists a state q for which R is true and fS(R) false. Let P1 be the predicate, which is true for the state q and false otherwise. There exists a healthy predicate transformer fK, such that $fK(P1) = Q$ and $fK(fS(R)) = F$. Because $P1 \Rightarrow R$, we have $Q = fK(P1) \Rightarrow fK(R)$, and so, by (1), $Q \Rightarrow E(fK(fS(R))) = E(F)$. Conversely, if $Q \Rightarrow E(F)$, clearly (1) is satisfied.

3. $R = F$. Then $fS(R) = F$, so $R \Rightarrow fS(R)$ holds and (1) is satisfied for all Q.

Remark. In order to give an example of a text K, such that the corresponding predicate transformer fK satisfies the requirements stated above, we assume for the sake of simplicity of writing that there is only one variable x and that a state is determined by the value of x. If H1 is a text to which corresponds the predicate transformer fSTOP and if the state q corresponds to x = a, in both cases 1. and 2. the following text may be chosen for K:

if Q **then** x := a **else** H1 **fi** .

We conclude, that Q and R satisfy (1) and not (2) iff
either $Q \Rightarrow E(F)$ holds and $R \Rightarrow fS(R)$ does not hold,
or $Q \Rightarrow E(Q)$ does not hold and $R = F$.

In the first of these two cases the conclusion of the invariance theorem is easily proved:

$$Q \text{ and } fH(T) \Rightarrow Q \Rightarrow E(F) \Rightarrow E(fH_0(fS(R))) = fH_1(R) \Rightarrow fH(R) \ .$$

The second case, however, leads to an exception for the invariance theorem. If R = F, (1) is satisfied for all Q and the conclusion of the theorem is equivalent with

$$Q \text{ and } fH(T) = F \ ,$$

which clearly needs not to hold.

In the course of the proof of the invariance theorem, a formula (18) on p.16 of EWD 372 is used, which reads

$$fH_j(T) \Rightarrow E(fH_{j-1}(T)) \ .$$

The following example is a counterexample for this formula.
Let x be an integer variable. Consider

$$\underline{\text{while}}\ x > 0\ \underline{\text{do}}\ x := x - 2\ \underline{\text{od}},$$

considered as a recursive procedure in the way this is done on p.17 of EWD 372. We choose predicates Q and R satisfying the requirements formulated on that page, viz. Q : "x is even" and R : "x is even and $x \leq 0$".
For an arbitrary predicate P we have:

$$E(P) = (x > 0 \text{ and } P_{x-2 \to x}) \text{ or } (x \leq 0 \text{ and } x \text{ is even}),$$

$$E(fH_{j-1}(T)) = (x > 0 \text{ and } fH_{j-1}(T)_{x-2 \to x}) \text{ or } (x \leq 0 \text{ and } x \text{ is even}),$$

$$fH_j(T) = (x > 0 \text{ and } fH_{j-1}(T)_{x-2 \to x}) \text{ or } (x \leq 0).$$

For x = -1, however, $fH_j(T)$ is true and $E(fH_{j-1}(T))$ is false.

In the proof of the invariance theorem the use of (18) may be replaced by the use of

$$(Q \text{ and } fH_j(T)) \Rightarrow E(fH_{j-1}(T)) \ ,$$

which we now proceed to prove under the hypothesis that $Q \Rightarrow E(Q)$ is satisfied.
To do this we introduce a transformer G assigning to every pair of predicates P1 and P2 a predicate G (P1,P2) such that

$$fH''(P) = G(fH'(fS(P)),P) \ .$$

This means that

$$E(P) = G(P,R) \ .$$

The transformer G has the property, that for every pair fH1 and fH2 of healthy predicate transformers the transformer fH3 defined by

$$fH3(P) = G(fH1(P),\ fH2(P))$$

is a healthy predicate transformer. From this property it is easy to deduce for arbitrary predicates P1, P2, P3, P4 :

$$G(P1 \ \underline{\text{and}}\ P2,\ P3 \ \underline{\text{and}}\ P4) = G(P1,\ P3) \ \underline{\text{and}}\ G(P2,\ P4) \ .$$

Moreover G enjoys the monotonicity property with respect to both of its variables. Now

$$(Q \ \underline{\text{and}}\ fH_j(T)) \Rightarrow (E(Q) \ \underline{\text{and}}\ G(fH_{j-1}(fS(T)),\ T))$$

$$\Rightarrow (G(Q,R) \ \underline{\text{and}}\ G(fH_{j-1}(T),\ T)) =$$

$$= G(Q \ \underline{\text{and}}\ fH_{j-1}(T),\ R) \Rightarrow G(fH_{j-1}(T),\ R) =$$

$$= E(fH_{j-1}(T)) \ .$$

Summarizing the results found thus far we may state that the gaps in the proof of the theorem are filled, except for the case R = F, but in that case the theorem may be false. It seems to be advisable to add $R \neq F$ to the hypotheses of the theorem.