When messages may crawl.

The last session of the Tuesday Afternoon Club was devoted to the question when what has been proved to be correct when viewed as "a telex system", can also be implemented as "a mail system". The original motivation was the following.

We consider a network in which a node can transmit messages to (some) other nodes, and the only things we postulate about message transmission are
1) no message arrives before it has been sent
2) each message sent arrives eventually.
A system with such message transmission properties was called "a mail system".

The idea was to try to partition the correctness proof of a mail system in the following way:
1) prove that the system would be correct when viewed as "a telex system" in which message transmission is instantaneous, i.e. the sending and receiving of a message is part of the same "point action"
2) show that the system satisfies the antecedents of some general Laws --as yet unknown to us-- stating when the correctness of a telex system implies the correctness of the corresponding mail system.

We spent the afternoon on pruning the problem and on collecting "evidence" by designing all sorts of telex systems allowing and not allowing replacement by mail transmission. On account of the evidence, some Laws were conjectured, some of these conjectures were refuted by counterexample, and finally a formal approach for tackling the problem was suggested, but by then I was too tired to pursue the matter any further. That is what I did the next day. Hence this note, which has been written with the hope of providing next week's session of the Tuesday Afternoon Club with an inspiring starting point.

* * *

Consider the following repetitive program as representative for a two-node telex system

```
{P} do B1C → S1C; S1D {P}                    (1)
     ▯ B2D → S2D; S2C {P}
    od
```

Here the top line represents a telex message from node C to node D , the bottom line represents a telex message in the opposite direction. The guard B1C depends only on variables belonging to node C , in S1C only variables belong to node C are accessed, in S1D only variables belonging to node D , and similarly for the next line. (In this model, the messages are essentially empty envelopes; allowing the envelopes to contain something was felt to be a minor complication that we could postpone for the time being.) As indicated, P is the corresponding invariant relation. As part of the correctness proof of (1) the theorems

$$P \ \underline{\text{and}}\ B1C \ \Rightarrow\ wp(\text{"}S1C;\ S1D\text{"},\ P) \tag{2}$$

$$P \ \underline{\text{and}}\ B2D \ \Rightarrow\ wp(\text{"}S2D;\ S2C\text{"},\ P) \tag{3}$$

have been established.

We decided that the following program would be representative for the corresponding mail system

```
{P} c, d := 0, 0 ;{M}
do B1C → S1C; d:= d + 1 {M}
 ▯ d > 0 → d:= d - 1; S1D {M}
 ▯ B2D → S2D; c:= c + 1 {M}
 ▯ c > 0 → c:= c - 1; S2C {M}
od
```

Here we have to prove

$$(c,\ d) \neq (0,\ 0)\ \underline{\text{or}}\ P = M \tag{4}$$

$$M\ \underline{\text{and}}\ B1C \ \Rightarrow\ wp(\text{"}S1C;\ d:= d + 1\text{"},\ M) \tag{5}$$

$$M\ \underline{\text{and}}\ d > 0 \ \Rightarrow\ wp(\text{"}d:= d - 1;\ S1D\text{"},\ M) \tag{6}$$

$$M\ \underline{\text{and}}\ B2D \ \Rightarrow\ wp(\text{"}S2D;\ c:= c + 1\text{"},\ M) \tag{7}$$

$$M\ \underline{\text{and}}\ c > 0 \ \Rightarrow\ wp(\text{"}c:= c - 1;\ S2C\text{"},\ M) \tag{8}$$

Relations (4), (6), and (8) can be satisfied independently of (2) and (3) by a suitable choice for M. Defining for any statement S and any natural number x

$$S\uparrow 0 \;=\; \text{skip} \tag{9}$$

$$S\uparrow(x+1) \;=\; \text{"}S\uparrow x;\ S\text{"} \tag{10}$$

we can satisfy relations (4), (6), and (8) by choosing for M

$$M:\quad c \geq 0 \ \underline{\text{and}}\ d \geq 0 \ \underline{\text{and}}\ wp(\text{"}S1D\uparrow d;\ S2C\uparrow c\text{"},\ P) \tag{11}$$

(Note that "S1D; S2C" = "S2C; S1D" : accessing disjoint sets of variables, they obviously commute.)

In the sequel we drop for the sake of brevity from (11) the (implied) terms $c \geq 0\ \underline{\text{and}}\ d \geq 0$. Trying to prove (5) using (2) I discovered that I had to make two further assumptions about node C

$$B1C \Rightarrow wp(S2C,\ B1C) \tag{12}$$

$$wp(\text{"}S2C;\ S1C\text{"},\ R) \Rightarrow wp(\text{"}S1C;\ S2C\text{"},\ R) \quad \text{for any } R \tag{13}$$

From (12) we immediately deduce for any $x \geq 0$

$$B1C \Rightarrow wp(\text{"}S2C\uparrow x\text{"},\ B1C) \qquad . \tag{14}$$

From (13) --which, for instance, would be satisfied if $S1C$ and $S2C$ were to commute-- we immediately deduce for any $x \geq 0$ and any R

$$wp(\text{"}S2C\uparrow x;\ S1C\text{"},\ R) \Rightarrow wp(\text{"}S1C;\ S2C\uparrow x\text{"},\ R) \qquad . \tag{15}$$

In order to prove (5), we now proceed as follows.

$$M\ \underline{\text{and}}\ B1C \;= \qquad \text{(by (11))}$$

$$wp(\text{"}S1D\uparrow d;\ S2C\uparrow c\text{"},\ P)\ \underline{\text{and}}\ B1C \;\Rightarrow \qquad \text{(by (14))}$$

$$wp(\text{"}S1D\uparrow d;\ S2C\uparrow c\text{"},\ P)\ \underline{\text{and}}\ wp(\text{"}S2C\uparrow c\text{"},\ B1C) \;=$$

$$wp(\text{"}S1D\uparrow d;\ S2C\uparrow c\text{"},\ P)\ \underline{\text{and}}\ wp(\text{"}S1D\uparrow d\ ;\ S2C\uparrow c\text{"},\ B1C) \;=$$

$$wp(\text{"}S1D\uparrow d;\ S2C\uparrow c\text{"},\ P\ \underline{\text{and}}\ B1C) \;\Rightarrow \qquad \text{(by (2))}$$

$$wp(\text{"}S1D\uparrow d;\ S2C\uparrow c\text{"},\ wp(\text{"}S1C;\ S1D\text{"},\ P)) \;=$$

$$wp(\text{"}S1D\uparrow(d+1);\ S2C\uparrow c;\ S1C\text{"},\ P) \;\Rightarrow \qquad \text{(by (15))}$$

$$wp(\text{"}S1C\text{"},\ wp(\text{"}S1D\uparrow(d+1);\ S2C\uparrow c\text{"},\ P)) \;= \qquad \text{(by (11))}$$

$$wp(\text{"}S1C;\ d{:=}\ d+1\text{"},\ M)$$

In this derivation only the last equality is fishy, because our form for M is most definitely not a first-order formula, and yet we appeal to the axiom of assignment. Yet I am sure that it is correct; the justification will require that the "variable" d does not occur in the original program (1). The 2nd and the 4th equalities depend on the disjointness of variables, the 3rd on the conjunction property of wp .

So much for the derived invariant relation. In order to complete the proof with a proof of convergence, we have to derive a new variant function as well, but that exercise is left for later.

In order to prove (7) from (3) we must make about node D the two assumptions analogous to (12) and (13) about node C .

* * *

The example is very modest, and in itself not very exciting. What does excite me is that the antecedent of our Law is formulated in local conditions only! Apparently the correctness proof of the telex system duly captures here all global aspects of the problem.

29th of March 1979

Plataanstraat 5
5671 AL NUENEN
The Netherlands

prof.dr.Edsger W.Dijkstra
Burroughs Research Fellow