When messages may crawl, II (A sequel to EWD708).

In EWD708 I wrote "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". The purpose of this note is to investigate how minor or major this complication turns out to be.

We modify the program by distinguishing the different messages from C to D by a subscript i and the ones in the opposite direction by a subscript j :

```
{P} do $B1C_i \rightarrow S1C_i;\ S1D_i$ {P}                    (1)
     [] $B2D_j \rightarrow S2D_j;\ S2C_j$ {P}
    od
```

and its correctness proof now comprises the (many) theorems

$$P \text{ \underline{and} } B1C_i \Rightarrow wp(\text{"}S1C_i;\ S1D_i\text{"},\ P) \qquad (2i)$$

$$P \text{ \underline{and} } B2D_j \Rightarrow wp(\text{"}S2D_j;\ S2C_j\text{"},\ P) \quad . \qquad (3j)$$

In this note we regard the way in which the difference between different messages from C to D has been indicated by the implementation as irrelevant: the contents of the messages may differ, they may be sent along different channels that can be distinguished, or any mixture thereof. It is an implementation detail, from which we are allowed to abstract.

In analogy to EWD708, the following program is regarded to be representative for the corresponding mail system:

```
{P} ($\underline{A}$ j: $c_j$:= 0); ($\underline{A}$ i: $d_i$:= 0); {M}
do $B1C_i \rightarrow S1C_i;\ d_i := d_i + 1$ {M}
 [] $d_i > 0 \rightarrow d_i := d_i - 1;\ S1D_i$ {M}
 [] $B2D_j \rightarrow S2D_j;\ c_j := c_j + 1$ {M}
 [] $c_j > 0 \rightarrow c_j := c_j - 1;\ S2C_j$ {M}
od
```

with the corresponding proof obligations

$(\underline{E}\ j\colon c_j \neq 0)\ \underline{\text{or}}\ (\underline{E}\ i\colon d_i \neq 0)\ \underline{\text{or}}\ P = M$ (4)

$M\ \underline{\text{and}}\ B1C_i \Rightarrow wp(\text{"}S1C_i;\ d_i := d_i + 1\text{"},\ M)$ (5i)

$M\ \underline{\text{and}}\ d_i > 0 \Rightarrow wp(\text{"}d_i := d_i - 1;\ S1D_i\text{"},\ M)$ (6i)

$M\ \underline{\text{and}}\ B2D_j \Rightarrow wp(\text{"}S2D_j;\ c_j := c_j + 1\text{"},\ M)$ (7j)

$M\ \underline{\text{and}}\ c_j > 0 \Rightarrow wp(\text{"}c_j := c_j - 1;\ S2C_j\text{"},\ M)$ (8j)

With the same notational convention --(9) and (10)-- from EWD708, we can satisfy (4), (6i), and (8j) by choosing for M

M: $wp(\text{"}(\underline{A}\ i\colon S1D_i \uparrow d_i);\ (\underline{A}\ j\colon S2C_j \uparrow c_j)\text{"},\ P)$ (11)

provided that (11) makes sense. In analogy to EWD708 this implies

$(\underline{A}\ j\colon c_j \geq 0)\ \underline{\text{and}}\ (\underline{A}\ i\colon d_i \geq 0)$,

but this invariance is duly maintained by the above representation of the mail system. But for (11) to make sense, we must require that $(\underline{A}\ i\colon S1D_i \uparrow d_i)$ and $(\underline{A}\ j\colon S2C_j \uparrow c_j)$ are defined, i.e. we must require

$(\underline{A}\ i1, i2\colon \text{"}S1D_{i1} \uparrow d_{i1};\ S1D_{i2} \uparrow d_{i2}\text{"} = \text{"}S1D_{i2} \uparrow d_{i2};\ S1D_{i1} \uparrow d_{i1}\text{"})$ (16)

and $(\underline{A}\ j1, j2\colon \text{"}S2C_{j1} \uparrow c_{j1};\ S2C_{j2} \uparrow c_{j2}\text{"} = \text{"}S2C_{j2} \uparrow c_{j2};\ S2C_{j2} \uparrow c_{j2}\text{"})$ (17)

(This curious way of numbering results from my desire to give similar formulae in this note and in EWD708 the same number.)

Salvo errore et omissione I have come to the conclusion that properties (12) and (13) are stronger than necessary, and so are their consequences (14) and (15), as mentioned in EWD708. In order to prove (5i) from (2i) the weaker assumptions

$(\underline{A}\ j\colon B1C_i \Rightarrow wp(\text{"}S2C_j \uparrow c_j\text{"},\ B1C_i))$ (14)

$\underline{\text{and}}$ $(\underline{A}\ j\colon B1C_i\ \underline{\text{and}}\ wp(\text{"}S2C_j \uparrow c_j;\ S1C_i\text{"},\ R) \Rightarrow wp(\text{"}S1C_i;\ S2C_j \uparrow c_j\text{"},\ R))$ (15)

suffice. (The absence of the beginning term "B1C" in (13) and (15) of EWD708 is, in retrospect, just an omission.)

One way of proving (14) and (15) is to show --as suggested in EWD708-- for each (i,j)-pair

$B1C_i \Rightarrow wp(\text{"}S2C_j\text{"},\ B1C_i)$ (12)

$$B1C_i \ \underline{\text{and}}\ wp(\text{"}S2C_j;\ S1C_i\text{"},\ R) \Rightarrow wp(\text{"}S1C_i;\ S2C_j\text{"},\ R) \quad . \qquad (13)$$

Properties (12) and (13) have the attraction that they are local properties of node C of the telex system. Note that relations (14) and (15) are also a consequence of

$$B1C_i \Rightarrow (c_j = 0) \quad . \qquad (18)$$

Similarly, in the spirit of EWD708, we would try to prove for any (j1,j2)-pair

$$\text{"}S2C_{j1};\ S2C_{j2}\text{"} = \text{"}S2C_{j2};\ S2C_{j1}\text{"} \qquad (19)$$

from which (17) follows. Again we should note the existence of the alternative: $c_{j1} = 0\ \underline{\text{or}}\ c_{j2} = 0$.

Summarizing our proof obligation with respect to node C , we have to show:

$$(\underline{A}\ i,\ j;\ B1C_i \Rightarrow wp(\text{"}S2C_j\text{"},\ B1C_i)\ \underline{\text{or}}\ c_j = 0) \qquad (20)$$

$$(\underline{A}\ i,\ j:\ B1C_i\ \underline{\text{and}}\ wp(\text{"}S2C_j;\ S1C_i\text{"},\ R) \Rightarrow wp(\text{"}S1C_i;\ S2C_j\text{"},\ R)\ \underline{\text{or}}\ c_j = 0)(21)$$

$$(\underline{A}\ j1,j2:\ \text{"}S2C_{j1};\ S2C_{j2}\text{"} = \text{"}S2C_{j2};\ S2C_{j1}\text{"}\ \underline{\text{or}}\ c_{j1} = 0\ \underline{\text{or}}\ c_{j2} = 0) \qquad (22)$$

With respect to node D we have, mutatis mutandis, the same obligations.

The weakening of our proof obligations, as represented by (20), (21), and (22) leaves me with mixed feeling. Each time we have to make essential use of the weakening, we have to prove that under certain circumstances "exponents" are zero, and those are global properties that are not directly reflected --at least for the time being I don't see how-- in the original telex system. I console myself with the thought that, if a mail system is our eventual target, they are not very desirable properties: in order to make a mail system it is customary to make message receptions commute if possible. One advantage of conditions (20), (21), and (22) is certainly that they give the designer of a mail system a clear summary of his options.

Plataanstraat 5
5671 AL NUENEN
The Netherlands

prof.dr.Edsger W.Dijkstra
Burroughs Research Fellow