A correction of EWD851b

Thanks to the scrutiny of F.E.J. Kruseman Aretz, an error in EWD851b was discovered, which is in urgent need of correction. The Tuesday Afternoon Club, in particular W.H.J. Feijen, designed a more convincing derivation of the correct invariant, and that is what is recorded in this note. (Feijen also convincingly argued that the rules of our formal game should be stated explicitly; I agree, but under the present circumstances the design of such a calculus has to be postponed.)

We search for the transitive closure of

(0) $\qquad (\text{wn u})^* \text{ Wn u}$

under the following list of transformations —with the numbering of EWD851b but in an order that suits our current purpose—

	wn u	$\rightarrow$	wd s	(n.1)
s	wn u	$\rightarrow$	u bn s	(s.0)
u	bn	$\rightarrow$	u bd	(n.2)
s	wd	$\rightarrow$	u bd	(s.1)
s	Wn u	$\rightarrow$	t wn u	(s.2)
	Wn u	$\rightarrow$	Wc u	(n.0)
	Wc u	$\rightarrow$	Wn u	(c.0)
s	Wc u	$\rightarrow$	u Bc u	(s.3)
u	Bc u	$\rightarrow$	t wn u	(c.1)
	wd t	$\rightarrow$	Wc u	(t.2)
u	bn t	$\rightarrow$	t wn u	(t.1)

$$u \; bd \; t \quad \rightarrow \quad u \; Bc \; u$$

The transitive closure of (0) under (n.1) is

(0') $\quad (wn\ u \mid wd\ s)^*\ Wn\ u$.

Since (i) the transitive closure of $s\ (wn\ u)^*$ under (s.0) equals $(u\ bn)^*\ s\ (wn\ u)^*$ and (ii) (0) can be rewritten as $(wn\ u \mid wd\ s\ (wn\ u)^*)^*\ Wn\ u$, the transitive closure of (0') under (s.0) equals

$$(wn\ u \mid wd\ (u\ bn)^* s\ (wn\ u)^*)^*\ Wn\ u$$

which can be simplified to

(1) $\quad (wn\ u \mid wd\ (u\ bn)^*\ s)^*\ Wn\ u$

which is also closed under (n.1).

The transitive closure of (1) under (n.2) is

(2) $\quad (wn\ u \mid wd\ (u\ bn \mid u\ bd)^*\ s)^*\ Wn\ u$

which we write as

(2) $\quad H^*\ Wn\ u$ $\qquad$ with
(3) $\quad H = wn\ u \mid Q\ s$ $\qquad$ with
(4) $\quad Q = wd\ (u\ bn \mid u\ bd)^*$.

and we note that the substrings H, H^*, and H^*Q are closed under the transitions considered so far. And so is (2), neither $H\ Wn$ nor $u\ H$ introducing the possibility of applying any of the transformations. Strings H, H^*, H^*Q and ring (2) are also closed under (s.1). The reason is that the substring $s\ wd$ can only occur in the substring $H\ Q$ of the form $Q\ s\ Q$, written out in full

$$wd\ (u\ bn \mid u\ bd)^*\ s\ \ wd\ (u\ bn \mid u\ bd)^* \quad .$$

Hence the only possible effect of (s.1) is to replace a string of the form Q s Q by one of the form Q .

Inclusion of the next transformation (s.2) is more complicated. In (2) we can make the only way in which the substring s Wn u can occur explicit by adding the superfluous term Q s Wn u :

$$H^* (\text{Wn u} \mid \text{Q s Wn u})$$

and we conclude that the transitive closure of (2) under (s.2) is

$$H^* (\text{Wn u} \mid \text{Q + wn u}) \quad ,$$

which is no longer closed under (n.1); that closure gives

$$H^* (\text{Wn u} \mid \text{Q + (wn u} \mid \text{wd s}))\quad .$$

In view of the structure of H and the fact that our expressions represent circular structures, this equals

$$H^* (\text{Wn u} \mid \text{Q + (wn u} \mid \text{wd s (wn u)}^*))$$

which yields under (s.0)

$$H^* (\text{Wn u} \mid \text{Q + (wn u} \mid \text{wd (u bn)}^* \text{s (wn u)}^*))$$

which yields under (n.2)

(5) $H^* (\text{Wn u} \mid \text{Q + H})$.

H^* Q and H H^* being closed under all transformations, (5) is closed under the transformations considered so far.

Closing (5) under the next transformation (n.0) yields

(6) $H^*(\text{Wn u} \mid \text{Wc u} \mid \text{Q} + \text{H})$,

which is closed under the transformations considered so far, and obviously under the next one (c.0) as well.

In order to accommodate (s.3), we observe that s Wc can only occur in the substring Q s Wc u, which can be added as superfluous term in which the substitution can be performed to construct the next

(7) $H^*(\text{Wn u} \mid \text{Wc u} \mid \text{Q} + \text{H} \mid \text{Q u Bc u})$

No further extensions are now required. Transformation (c.1) can only transform Q u Bc u, which becomes Q + wn u, a special case of the preceding alternative. Q + H is either of the form wd + H or not. In the former case the next transformation (t.2) may transform it into Wc u H, a case subsumed by the previous alternative (thanks to the circularity). Otherwise Q + H is of the form Q u bn + H or of the form Q u bd + H. Transformation (t.1) generates from the former Q + wn u H, subsumed by Q + H, transformation (t.0) transforms the latter into Q u Bc u H, which is subsumed in the last alternative.

* * *

The above derivation is not as calculational as we would like it to be; the development of the calculus is something for later.

One remark about the number of elements in the string. Our regular expressions define a language of strings of arbitrary lengths. For a circular arrangement of a given number of machines, only those strings that are of the appropriate length are applicable. Some machine or ring states and some transformations cannot occur if the ring is too small, but this does not contradict our claim that we are deriving the strongest invariant in the sense that each string of the language may occur.

Plataanstraat 5
5671 AL NUENEN
The Netherlands

13 April 1983
prof. dr. Edsger W. Dijkstra
Burroughs Research Fellow