Triggered by Higman's Lemma

This EWD is devoted to a proof of Higman's Lemma, because we tried to prove the latter, but failed.

For finite strings of characters from an alphabet we define the length # and the subsequence relation $\sqsubseteq$ (in the style of SASL) by

$$\begin{array}{lll} \#[\,] & = & 0 \\ \#(a:x) & = & 1 + \#x \\ [\,] \sqsubseteq x & = & true \\ (a:x) \sqsubseteq [\,] & = & false \\ (a:x) \sqsubseteq (b:y) & = & \textbf{if}\ a = b \rightarrow x \sqsubseteq y \qquad (*) \\ & & [\!]\ a \neq b \rightarrow (a:x) \sqsubseteq y \qquad (**) \\ & & \textbf{fi} \end{array}$$

(It follows —though we shall neither use nor prove it here— that $\sqsubseteq$ is a partial order, i.e. reflexive, transitive, and antisymmetric.)

We now consider possibly infinite sequences of finite strings (or, if you prefer, functions of type: nat → string) and define on them the predicates "tight" and "bad":

$$tight.s \;\equiv\; \langle \forall i,j : 0 \le i \wedge i < j : (\#s.i \le \#s.j) \wedge \neg(s.i \sqsubseteq s.j) \rangle$$

$$bad.s \;\equiv\; tight.s \wedge (s \text{ is infinite})$$

Higman's Lemma states that there are no

bad sequences if the string characters are taken from a finite alphabet.

* * *

We shall prove the contrapositive, i.e. we shall show how the existence of bad sequences implies that the alphabet is infinite. This is done in 2 steps. In the first step we show the existence of a "minimal bad sequence" t, i.e. a bad sequence t such that

(0) $\langle\forall s: bad.s: \langle\forall k: 0\le k: s\uparrow k = t\uparrow k \Rightarrow \#s.k \ge \#t.k\rangle\rangle$,

in which "$..\uparrow k$" denotes the prefix of length k. In the second step we show that each character of the alphabet is the leading character of at most a finite number of strings in t; hence, t being an infinite sequence of strings, the alphabet is infinite.

The existence of a bad sequence t satisfying (0) is demonstrated by mathematical induction. Consider the induction hypothesis that $t\uparrow n$ satisfies

$$\langle\forall s: bad.s: \langle\forall k: 0\le k< n: s\uparrow k = t\uparrow k \Rightarrow \#s.k \ge \#t.k\rangle\rangle$$
$$\wedge \langle\exists s: bad.s: s\uparrow n = t\uparrow n\rangle \quad .$$

For $n=0$, the first conjunct is vacuously true and the second conjunct reduces to $\langle\exists s:: bad.s\rangle$, i.e. to the antecedent.

For the step from $n=N$ to $n=N+1$, we leave $t\uparrow N$ as it is, and define $t.N$ by $t.N = z.N$, where z satisfies

$$bad.z \wedge z\uparrow N = t\uparrow N \wedge \langle \forall s : bad.s : s\uparrow N = t\uparrow N : \#s.N \geq \#z.N \rangle .$$

The second conjunct of the hypothesis for $n=N$, viz. $\langle \exists s : bad.s : s\uparrow N = t\uparrow N \rangle$ ensures the existence of at least one such z, the choice ensures the invariance of the induction hypothesis under $n:=n+1$. (For the second conjunct, $s=z$ is a witness.) Hence there exists a t that satisfies the induction hypothesis for all n, and hence —from the first conjunct— satisfies (0). That t is a bad sequence follows from it being infinite and the second conjunct:

$$\begin{array}{ll} & \langle \forall n :: \langle \exists s : bad.s : s\uparrow n = t\uparrow n \rangle \rangle \\ \Rightarrow & \quad \{\text{the prefix of a bad sequence is tight}\} \\ & \langle \forall n :: tight.(t\uparrow n) \rangle \\ = & \quad \{\text{def. of tight, of } \uparrow \text{ and predicate calculus}\} \\ & tight.t \end{array}$$

And this completes the first step.

For the second step we consider a character b that occurs as first character of a string in t. Let u be the (non-empty) subsequence of t obtained by removing from t all strings whose first character differs from b. Our task is to show that u is finite.

We define h to be the smallest value such

that $t.h$ starts with a b ; then $u.0 = t.h$.
We define v as the sequence obtained from u by removing from each string in u the first character. We remark

- $\# v.0 = \# t.h - 1$
- because u is a subsequence of t , it is tight, and therefore v is tight (on account of (*): all strings of u start with the same b , which is removed from all of them)
- showing that u is finite means showing that v is finite.

Let m be the minimum value such that $\# t.m = \# t.h$. Because t is tight, $m \leq h$. Define sequence w as $t{\uparrow}m$, followed by v . We observe

- $t{\uparrow}m$ is tight (subsequence of t)
- v is tight (see above)
- because of the definition of m , all strings in $t{\uparrow}m$ have lengths less than $\# t.h$, i.e. at most $\# v.0$; in short
  $$0 \leq i \wedge i < j \Rightarrow \# w.i \leq \# w.j \quad .$$
- because $m \leq h$, also in the case
  $0 \leq i < m \wedge m \leq j$ we have $\neg (w.i \sqsubseteq w.j)$, now on account of (**): $w.i$ is a $t.i$ of the form $a{:}x$ with $a \neq b$, $w.j$ is of the form y, with $b{:}y$ occurring higher up in t ; in short,
  $$0 \leq i \wedge i < j \Rightarrow \neg (w.i \sqsubseteq w.j)$$
- combining the last two observations, we conclude that w is tight .

- showing that v is finite means showing that w is finite.

About w we observe

- $w\!\uparrow\!m = t\!\uparrow\!m$ (by construction)
- $\#w.m < \#t.m$ ($\#w.m = \#v.0$, $\#v.0 = \#t.h - 1$, $\#t.h = \#t.m$)

Confronting these two observations with (0), we conclude $\neg\, bad.w$; because of $tight.w$, we conclude that w is finite. QED

* * *

As confessed, we missed this proof. We tried to prove that a nondeterministic algorithm building a tight sequence would terminate and vainly searched for an ordering for which the well-foundedness could be shown in a familiar manner. It was probably that last constraint that did us in.

We did write down the formal definition of $\sqsubseteq$ and were very aware of the immediate consequences of (*) and (**). Following an old habit, we built up a little theory about $\sqsubseteq$, viz. that $\sqsubseteq$ is a partial order, missing the hint that the relation occurring in "tight" is $\not\sqsubseteq$.

The central invention in the above proof is the minimal bad sequence t . Again, I blame myself for not having thought of it. The exploitation of an existential quantification in an antecedent for the construction of a special —usually in some sense extreme— witness is a wellknown device, and I knew it. But I did not think of it. Perhaps we should invent a catchy name for it.

The decision, taken on EWD1111-1, to prove the contrapositive was not necessary: a weakening chain showing $P \Rightarrow Q$ can be translated (by <u>syntactic</u> transformation) into a strengthening chain showing $\neg P \Leftarrow \neg Q$.

I am grateful to David Gries for having brought Higman's Lemma to my attention, and to the members of the ATAC, J.R. Rao in particular, for having discussed this problem with me.

Austin, 23 October 1991

prof. dr. Edsger W. Dijkstra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712-1188
USA