Applications of the length function theorem

Recall that we studied programs over well-structured domains

$$(\Sigma, COM, [\![-]\!])$$

where
- the set of states Σ can be endowed with a wpo $\leq$ so that
- $\leq$ is a simulation for all $[\![com]\!]$.

Such programs have a semantics in terms of well-structured transition systems

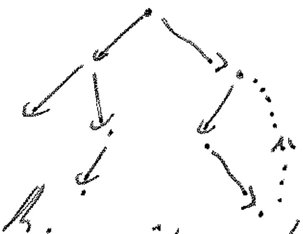
$$(S, \rightarrow, \leq)$$

whose
- set of states $(S, \leq)$ is a wqo
- where $\leq$ is a simulation wrt. $\rightarrow$.

<u>Now</u>: We assume $(S, \leq, |.|)$ is even an nwqo.

Termination:

Recall that we can decide termination of WSTS by computing the reachability tree and returning "does not terminate" when we encounter a repetition along a path.



Let $s_0 \in S$ be an initial state.

Let $n = |s_0| + 1$.

Let $g(|s|)$ be an upper bound on the space needed to compute and write down a successor $s \rightarrow s'$.

We expect g to be increasing.
With these requirements, we can use g as the control function and invoke the length function theorem to obtain an upper bound
$$f(n) \geq L_{g,s}(n).$$

<u>Remark:</u>

- Once we know f, we can change the algorithm.
  We just look for a <u>witness</u> of <u>non-termination</u>.
  This is a path
  $$s_0 \to s_1 \to \dots \to s_\ell$$
  of length $\boxed{\ell = f(n) + 1}$.
  Note that we no longer check for repetitions.
  Why does this work?
  Since bad sequences can be at most $f(n)$-long, a sequence of length $f(n)+1$ has to be good.

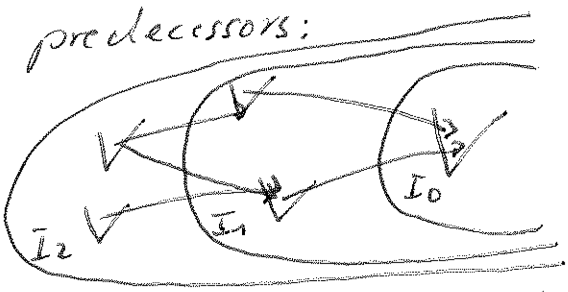
- Assume g is honest, meaning $g(n)$ can be computed in time/space elementary in $g(n)$.
  Also assume f is honest.
  The above now yields a non-deterministic algorithm that works in space elementary in $g^\ell(n) = g^{f(n)+1}(n)$.
  Honesty is needed to initialize a counter that is needed to enforce termination.
  One can show that $g^{f(n)+1}(n)$ is the same $\mathcal{F}_k$-class that also $f(n)$ belongs to.

Coverability / control-state reachability / upward-closed reachability

Recall that we are able to decide the reachability of an upward-closed set $I_0 \subseteq S$ in a WSTS.

We simply saturate the set of predecessors:

$$I_1 = pre(I_0) \cup I_0$$
$$I_2 = pre(I_1) \cup I_1$$
$$\vdots$$



Either we find the initial state, then we return "reachable", or we converge unsuccessfully, then we return "unreachable".

Also recall that we need to represent upward-closed sets by their minimal elements.

- To estimate the complexity, assume $I_0 = \{t\}\uparrow$, we want to cover precisely one state, say from s.

How long can a sequence

$$\{t\}\uparrow = I_0 \subsetneq I_1 \subsetneq \ldots \subsetneq I_\ell \quad \text{with } s \in I_\ell \setminus I_{\ell-1}$$

be, where we only find s in the last set I_ℓ?

Since the sequence does not stabilize, there are minimal elements s_i in $I_i \setminus I_{i-1}$.

There is such a minimal element s_ℓ in $I_\ell \setminus I_{\ell-1}$ with $s_\ell \leq s$, and there are no such elements in the sets I_i before.

We consider the sequence $(*)$.

$$s_1 s_2 \ldots s_\ell$$

We have $s_i \not\leq s_j$ for $i \leq j$, otherwise $s_j \in I_i$.

Hence, the sequence is bad.

How long can the sequence be?

We first have to control it.

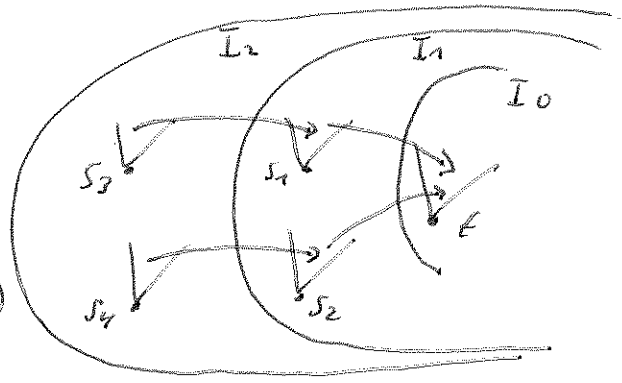
We do <u>not</u> have $s_i \to s_{i+1}$.

We have to consider the sets of minimal elements in the I_i,
and give a bound that holds for all sequences (*) we could form.

Actually, the maximal length of such a sequence is the same as the maximal length of a sequence where the elements are predecessors as follows:

$$s_{i+1} \in pb(s_i) = \min(pre(\{s_i\}\uparrow)).$$

<u>Illustration</u>:



- The sequence $t.s_1.s_4$ is of the form (*) but s_4 is <u>not</u> a pb-predecessor of s_1.
- The sequences $t.s_2.s_4$ and $t.s_1.s_3$ have the same length and satisfy the pb-requirement.

Assume
- $s' \leq s$ can be checked in space elementary in $|s'|+|s|$.
- $pb(s')$ can be computed in space $g(|s'|)$ for an increasing g.

Then $\ell \leq L_{g,s}(|t|+1)$.

<u>Remark</u>:

We can again devise a non-deterministic algorithm that looks for a <u>witness</u>

$t = s_0' . s_1' \ldots s_\ell' \le s$ with $s_{i+1}' \in pb(s_i')$.

Assume g is honest.
Assume f is honest and bounds $L_{g,s}$.
Since each s_i' satisfies $|s_i'| \le g^{f(|t|+1)}(|t|+1)$,
the algorithm works in space elementary in
$g^{f(|t|+1)}(|t|+1) + |s|$.