

PROBLEM SHEET 7

Alex Kavvos

The following questions are about Modernised Algol.

1. Write down a transition sequence that begins with the following command-store pair, and ends in a final state, where $\text{one} \stackrel{\text{def}}{=} \text{succ}(\text{zero})$ as usual. Moreover, show that the command is ok with $\Sigma \stackrel{\text{def}}{=} a$.

$$\{a := \text{zero}; \text{decl } b := \text{one in } \{x \leftarrow @b; \text{ret } x\}\} \parallel \{a \mapsto \text{one}\}$$

2. Complete the proofs of progress and preservation for Modernised Algol. As usual, do this in steps: first formulate a canonical forms lemma; then prove a substitution lemma; and then progress and preservation themselves.

You are going to need the following ‘extension’ lemma.

Lemma 1 (Extension).

- If $\Gamma \vdash_{\Sigma} e : \tau$ then $\Gamma \vdash_{\Sigma, \Sigma'} e : \tau$ for any appropriate Σ' .
- If $\Gamma \vdash_{\Sigma} m \text{ ok}$ then $\Gamma \vdash_{\Sigma, \Sigma'} m \text{ ok}$ for any appropriate Σ' .

The word ‘appropriate’ here means that the locations in Σ' do not clash with any of the locations in Σ . The Barendregt convention also means that any bound locations in e or m should be ‘automatically’ renamed to avoid clashing with Σ' .

You are also going to need the following ‘mobility’ lemma.

Lemma 2 (Mobility). If $\vdash_{\Sigma} e : \text{Nat}$ and $e \text{ val}$ then $\vdash_{\emptyset} e : \text{Nat}$.

This holds by repeated applications of canonical forms for Nat: if e is a value of natural number type it must be of the form $\text{succ}^n(\text{zero})$ for some $n \in \mathbb{N}$. Hence, starting with the typing rule ZERO with $\Sigma = \emptyset$ and repeatedly applying Succ we can show that $\vdash_{\emptyset} e : \text{Nat}$.

Finally, the substitution lemma you will need to prove (or assume!) is the following:

Claim 3 (Substitution).

- If $\Gamma \vdash_{\Sigma} v : \sigma$, and $\Gamma, x : \sigma \vdash_{\Sigma} e : \tau$ then $\Gamma \vdash_{\Sigma} e[v/x] : \tau$.
- If $\Gamma \vdash_{\Sigma} v : \sigma$, and $\Gamma, x : \sigma \vdash_{\Sigma} m \text{ ok}$, then $\Gamma \vdash_{\Sigma} m[v/x] \text{ ok}$.

We may be using the letter v , but it need not be a value.

[For preservation, perform a simultaneous induction on $e \mapsto e'$ and $m \parallel \mu \mapsto_{\Sigma} m' \parallel \mu'$. Do a similar simultaneous induction on typing derivations for progress. You will need to use the canonical forms lemma in both, not just when proving progress.]