A Appendix

Theorem 1 (Well-Definedness). *A program p either reduces to a value v; starts an infinitely long chain of reductions; or reduces to* `exn`.

Proof. The reduction relation satisfies unique decomposition, which means that an expression is either a value, `exn`, or it can be uniquely partitioned into an evaluation context and a $\rightarrow$ redex or `exn`. Using a progress-and-preservation approach, we can then prove that this subject is preserved across all reductions.

Lemma 1 (Preservation: $\rightarrow$). *If $\widehat{\rho} \models_e e$ and $e \rightarrow e'$, then $\widehat{\rho} \models_e e'$.*

Proof. By cases on $\rightarrow$, using the corresponding analysis rules.

Corollary 1 (Preservation: $\longmapsto$). *If $\widehat{\rho} \models_e e$ and $e \longmapsto e'$, then $\widehat{\rho} \models_e e'$.*

Theorem 2 (Soundness). *For all $\widehat{\rho} \models p$, $p = d \ldots e$, if $e \longmapsto\!\!\!\!\rightarrow_{d\ldots} E[v^\ell]$, $\widehat{v} \in \widehat{\rho}(\ell)$.*

Proof. By induction on the length of $\longmapsto\!\!\!\!\rightarrow$, using Corollary 1.

Lemma 2. *If $(\widehat{\rho}, \widehat{\mathcal{D}}, \widehat{\mathcal{S}}, \widehat{\mathcal{F}}) \models p$, then $\xi[\![\widehat{\rho}]\!]_{\varphi[\![p]\!]_{\widehat{\rho}\widehat{\mathcal{D}}\widehat{\mathcal{S}}\widehat{\mathcal{F}}}} \models \varphi[\![p]\!]_{\widehat{\rho}\widehat{\mathcal{D}}\widehat{\mathcal{S}}\widehat{\mathcal{F}}}$.*

Proof. Let $\widehat{\rho}' = \xi[\![\widehat{\rho}]\!]_{\varphi[\![p]\!]_{\widehat{\rho}\widehat{\mathcal{D}}\widehat{\mathcal{S}}\widehat{\mathcal{F}}}}$. Proceed by cases on the result of $\varphi_e[\![e^\ell]\!]_{\widehat{\rho}\widehat{\mathcal{D}}\widehat{\mathcal{S}}\widehat{\mathcal{F}}}$, where e is a subexpression in p. We drop the subscript arguments of φ_e for conciseness.

- If $\varphi_e[\![e^\ell]\!] = (\texttt{delay}^* \; \varphi_e[\![e]\!]^\ell)^{\ell_1}$, by the [*delay*] analysis rule, three constraints must hold:
  1. $(\texttt{delay}^* \; \ell) \in \widehat{\rho}'(\ell_1)$
  2. $\widehat{\rho}' \models_e \varphi_e[\![e]\!]^\ell$
  3. $\widehat{\rho}'(\ell) \subseteq \widehat{\rho}'(\ell_1)$

  Constraints 1 and 3 hold by ξ, part (2). For constraint 2, we know from (†) in φ_e and the analysis rules that an environment satisfying $\varphi_e[\![e]\!]$ has `delay`* values that may not be in $\widehat{\rho}$. However, we also see that any inserted `delay`*s in $\varphi_e[\![e]\!]$ is exactly tracked by corresponding `darg` values in $\widehat{\rho}$. Thus constraint 2 holds as well, due to part (1) of ξ.
- If $\varphi_e[\![e^\ell]\!] = (\texttt{force} \; \varphi_e[\![e]\!]^\ell)^{\ell_1}$, by the [*force*] analysis rule, two constraints must hold:
  1. $\widehat{\rho}' \models_e \varphi_e[\![e]\!]^\ell$
  2. $\forall \widehat{v} \in \widehat{\rho}'(\ell), \widehat{v} \notin \texttt{delay} : \widehat{v} \in \widehat{\rho}'(\ell_1)$

  Constraint 1 holds by the same reasoning as in the `delay`* case, using (‡) in φ_e, and constraint 2 holds by part (3) of ξ's definition.
- All the other cases follow similar reasoning.

Theorem 3 (Safety). *For all $(\widehat{\rho}, \widehat{\mathcal{D}}, \widehat{\mathcal{S}}, \widehat{\mathcal{F}}) \models p$, if $\varphi[\![p]\!]_{\widehat{\rho}\widehat{\mathcal{D}}\widehat{\mathcal{S}}\widehat{\mathcal{F}}} = p' = d \ldots e$, then $e \not\longmapsto\!\!\!\!\rightarrow_{d\ldots}$* `dexn`*, and $e \not\longmapsto\!\!\!\!\rightarrow_{d\ldots}$* `dexn`*.

Proof. Let $\widehat{\rho}' = \xi[\![\widehat{\rho}]\!]_{\varphi[\![p]\!]_{\widehat{\rho}\widehat{\mathcal{D}}\widehat{\mathcal{S}}\widehat{\mathcal{F}}}}$. By lemma 2, $\widehat{\rho}' \models p'$.

1. Since `dexn` can only be generated if a `delay` value appears in a strict position, it is sufficient to show:

   $$e \not\longmapsto\!\!\!\rightarrow_{d...} E[S[(\texttt{delay}\ e_1^{\ell_1})^{\ell}]]$$

   We prove the claim by contradiction.
   Suppose $e \longmapsto\!\!\!\rightarrow_{d...} E[S[(\texttt{delay}\ e_1^{\ell_1})^{\ell}]]$. By soundness (theorem 2) applied to $\widehat{\rho}'$ and p', $(\texttt{delay}\ \ell_1) \in \widehat{\rho}'(\ell)$. Then from the definition of ξ, $(\texttt{delay}\ \ell_1) \in \widehat{\rho}(\ell)$. From the analysis rules in section 3, since we are at a strict position, a `delay` in $\widehat{\rho}(\ell)$ implies $\ell \in \widehat{\mathcal{F}}$, so φ would have inserted a `force` around ℓ. However, $\texttt{force}\ [\,] \notin S$ so we have a contradiction.
2. Since $\texttt{dexn}^*$ can only be generated if a $\texttt{delay}^*$ value appears in a strict position, it is sufficient to show:

   $$e \not\longmapsto\!\!\!\rightarrow_{d...} E[S[(\texttt{delay}^*\ e_1^{\ell_1})^{\ell}]]$$

   We prove the claim by contradiction.
   Suppose $e \longmapsto\!\!\!\rightarrow_{d...} E[S[(\texttt{delay}^*\ e_1^{\ell_1})^{\ell}]]$. By soundness (theorem 2), $(\texttt{delay}^*\ \ell_1) \in \widehat{\rho}'(\ell)$. Then from the definition of ξ, $(\texttt{darg}\ \ell_1) \in \widehat{\rho}(\ell)$. From the analysis rules in section 3, since we are at a strict position, $(\texttt{darg}\ \ell_1) \in \widehat{\rho}(\ell)$ implies $(\ell, \ell_1) \in \widehat{\mathcal{F}}$. From the definition of φ, the existence of $(\texttt{delay}^*\ e_1^{\ell_1})$ also implies that $e_1^{\ell_1}$ is an argument in a function call and that $\ell_1 \in \widehat{\mathcal{D}}$ and $\ell_1 \notin \widehat{\mathcal{S}}$. Finally, since $(\ell, \ell_1) \in \widehat{\mathcal{F}}$, $\ell_1 \in \widehat{\mathcal{D}}$, and $\ell_1 \notin \widehat{\mathcal{S}}$, φ would have inserted a `force` around ℓ. However, $\texttt{force}\ [\,] \notin S$, so we have a contradiction.