Non-determinism Analyses in a Parallel-Functional Language: Detailed Proofs

RICARDO PEÑA and CLARA SEGURA
Facultad de Informática, Universidad Complutense de Madrid
C/Juan del Rosal, nº 8, 28040 Madrid, Spain
(e-mail: ricardo@um.es, csegura@um.es)

Proof of Proposition 4
This proposition can be proved by structural induction on e. Let \( W^t \) : \( D_{2t} \rightarrow D_{2t} \)
be a widening operator for each type \( t \). All the cases but the recursive \texttt{let} expression
can be easily proved by using the hypothesis over the environments, the induction
hypothesis and the monotonicity properties of \( \phi_t \) and \( \mu_t \), proved in (Peña & Segura,
2001). So, here we only look at the recursive \texttt{let} expression.

Let \( e = \texttt{let rec} \{ v_i = e_i \} \text{ in } e' :: t \), where \( e' :: t, \) and each \( v_i \) and \( e_i \) have type \( t_i \).
On the one hand
\[
\llbracket e \rrbracket_2 \rho_2 = \llbracket e' \rrbracket_2 \bigcup_{n \in \mathbb{N}} (\lambda \rho_2. \rho_2 [v_i \rightarrow \llbracket e_i \rrbracket_2 \rho_2])^n(\rho_0) \]

where \( \rho_0 \) is the initial environment where each variable \( y :: t_y \) has \( \perp_{t_y} \) as abstract value (that is, the infimum of the corresponding domain). Let \( F \) be the function between environments \( \lambda \rho_2. \rho_2 [v_i \rightarrow \llbracket e_i \rrbracket_2 \rho_2] \). Let \( \rho_2^{\text{fix}} \) be \( \bigcup_{n \in \mathbb{N}} F^n(\rho_0) \).

On the other hand
\[
\llbracket e \rrbracket_3^{\text{fix}} = \llbracket e' \rrbracket_3^{\text{fix}} \bigcup_{n \in \mathbb{N}} (\lambda \rho_2. \rho_3 [v_i \rightarrow W^t_i (\llbracket e_i \rrbracket_3^{\text{fix}} \rho_2)])^n(\rho_0) \]

where \( \rho_0 \) is the initial environment where each variable \( y :: t_y \) has \( \perp_{t_y} \) as abstract value (that is, the infimum of the corresponding domain). Let \( G \) be the function between environments \( \lambda \rho_2. \rho_3 [v_i \rightarrow W^t_i (\llbracket e_i \rrbracket_3^{\text{fix}} \rho_2)] \). Let \( \rho_2^{\text{fix}} \) be \( \bigcup_{n \in \mathbb{N}} G^n(\rho_0) \).

If we proved that for each variable \( y :: t_y, \rho_2^{\text{fix}}(y) \subseteq \rho_3^{\text{fix}}(y) \), then by induction hypothesis we would have that
\[
\llbracket e \rrbracket_2 \rho_2^{\text{fix}} \subseteq \llbracket e' \rrbracket_3^{\text{fix}} \rho_2^{\text{fix}}
\]
which is what we want to prove. Let us see that for each \( n \geq 0 \), the following holds:

\[
\forall y :: t_y. (F^n(\rho_0))(y) \subseteq (G^n(\rho_0))(y)
\]

If this were true then
\[
\forall y :: t_y. (\bigcup_{n \in \mathbb{N}} F^n(\rho_0))(y) \subseteq (\bigcup_{n \in \mathbb{N}} G^n(\rho_0))(y)
\]
and we would be done. It can be proved by induction on \( n \):

- \( n = 0 \). This is a trivial case as \( F^0(\rho_0) = \rho_0, G^0(\rho_0) = \rho_0 \), which are equal.
\[ n = m + 1. \text{ Then} \]
\[
F^{m+1}(\rho_2) = F(F^m(\rho_2)) = \rho_2 \left[ e_i \mapsto [e_i^1_2](F^m(\rho_2)) \right] \quad \{ \text{by definition of } F \}
\]
and
\[
G^{m+1}(\rho_3) = G(G^m(\rho_3)) = \rho_3 \left[ e_i \mapsto \mathcal{W}_i(\{e_i^3_3\}(G^m(\rho_3))) \right] \quad \{ \text{by definition of } G \}
\]

Let \( y : t_y \). We want to prove that \((F^{m+1}(\rho_2))(y) \subseteq (G^{m+1}(\rho_3))(y)\). We distinguish two cases. If \( y \) is not any of the \( e_i \), then it holds by the hypothesis over the environments \( \rho_2 \) and \( \rho_3 \). If it is one of the \( e_i \), then we have to prove that
\[
[e_i^1_2](F^m(\rho_2)) \subseteq \mathcal{W}_i'(\{e_i^3_3\}(G^m(\rho_3)))
\]
This holds by induction hypothesis and by the hypothesis on \( \mathcal{W}_i' \):
\[
[e_i^1_2](F^m(\rho_2)) \subseteq [e_i^3_3](G^m(\rho_3)) \subseteq \mathcal{W}_i'(\{e_i^3_3\}(G^m(\rho_3)))
\]

\[ \square \]

**Proof of Proposition 5**
This proof is very similar to the previous one. The same steps can be followed in the recursive \( \text{let} \) expression, being now
\[
F = \lambda \rho_2. \rho_3 \left[ e_i^1 \mapsto \mathcal{W}_i'(\{e_i^3_3\}(\rho_3)) \right]^n(\rho_3)
\]
and
\[
G = \lambda \rho_2. \rho_3 \left[ e_i^1 \mapsto \mathcal{W}_i'(\{e_i^3_3\}(\rho_3)) \right]^n(\rho_3)
\]
The same induction on \( n \) is done, and at the end we have to prove that
\[
\mathcal{W}_i'(\{e_i^3_3\}(F^m(\rho_2))) \subseteq \mathcal{W}_i'(\{e_i^3_3\}(G^m(\rho_3)))
\]
which is true by induction hypothesis, \( \mathcal{W}_i \subseteq \mathcal{W}_i' \) and monotonicity of \( \mathcal{W}_i' \) (proved in (Peña & Segura, 2001)):
\[
\mathcal{W}_i'(\{e_i^3_3\}(F^m(\rho_2))) \subseteq \mathcal{W}_i''(\{e_i^3_3\}(F^m(\rho_2)))
\]

\[ \square \]

**Proof of Proposition 6**
This proposition can be proved by structural induction on \( t \).

- \( t = K \).
  - \((\Rightarrow)\). If \( z = n \), then trivially \( \alpha_s(s) \subseteq n \), as \( n \) is the top of Basic.
    If \( z = d \), then if \( s \in \Gamma_K(d) \), by definition of \( \Gamma_i \), we have that \( \text{unit}(s) \) is true, which implies that \( \alpha_s(s) = d \) by definition of \( \alpha_i \).
  - \((\Leftarrow)\). If \( z = d, \alpha_s(s) \subseteq d \) implies \( \text{unit}(s) \), so \( s \in \Gamma_K(d) \) by definition of \( \Gamma_i \).
    If \( z = n \), then trivially \( s \in \Gamma_K(n) = P(A_K) \).
Non-determinism Analyses

- $t = (t_1, \ldots, t_m)$.
  
  \[
s_1, \ldots, s_m \in \Gamma_t(z_1, \ldots, z_m)
  \]
  
  $\Leftrightarrow \forall i \in \{1, \ldots, m\}, \alpha_t(s_i) \subseteq z_i$
  
  \{by definition of $\Gamma_t$\}
  
  $\Leftrightarrow \alpha_t(s_1, \ldots, s_m) \subseteq (z_1, \ldots, z_m)$
  
  \{by definition of $\alpha_t$\}

- $t = \top$.
  
  \(-\) If $z = n$, then trivially $\alpha_t(s) \subseteq n$, as $n$ is the top of Basic.
  
  If $z = d$, then if $s \in \Gamma_T(d)$, by definition of $\Gamma_t$, we have that $det_T(s)$ which implies that $\alpha_T(s) = d$ by definition of $\alpha_t$.
  
  \(-\Rightarrow\). If $z = d$, $\alpha_T(s) \subseteq d$ implies $det_T(s)$, so $s \in \Gamma_T(d)$ by definition of $\Gamma_t$.
  
  If $z = n$, then trivially $s \in \Gamma_T(n) = \mathcal{P}(A_T)$.

- $t = t_1 \rightarrow t_2$.

  \(-\Rightarrow\). Let $f \in \Gamma_t(f^\#)$. Then,

  \[
  \forall s \in A_{t_1}, \alpha_{t_2}(f(s)) \subseteq f^\#(\alpha_{t_1}(s)) \quad (1)
  \]

  Let $z \in D_{2t_1}$. We have to prove that $\alpha_{t_2}(f(z)) \subseteq f^\#(z)$. By definition,

  \[
  \alpha_T(f(z)) = \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)).
  \]

  If $s_1 \in \Gamma_{t_1}(z)$, then by (1) $\alpha_{t_2}(f(s_1)) \subseteq f^\#(\alpha_{t_1}(s_1))$. So

  \[
  \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)) \subseteq f^\#(\alpha_{t_1}(s_1)) \quad (2)
  \]

  But, by induction hypothesis on $t_1$, if $s_1 \in \Gamma_{t_1}(z)$ then $\alpha_{t_1}(s_1) \subseteq z$, so by (2) and monotonicity of $f^\#$ we have that $\bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)) \subseteq f^\#(z)$.

  \(-\Rightarrow\). If $\alpha_t(f) \subseteq f^\#$, then by definition of $\alpha_t$,

  \[
  \forall z \in D_{2t_1}, \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)) \subseteq f^\#(z) \quad (3)
  \]

  Let $s \in A_{t_1}$. We have to prove that $\alpha_{t_2}(f(s)) \subseteq f^\#(\alpha_{t_1}(s))$.

  As $\alpha_{t_1}(s) \in D_{2t_1}$, by (3) we have that $\bigsqcup_{s_1 \in \Gamma_{t_1}(\alpha_{t_1}(s))} \alpha_{t_2}(f(s_1)) \subseteq f^\#(\alpha_{t_1}(s))$.

  By induction hypothesis, trivially $s \in \Gamma_{t_1}(\alpha_{t_1}(s))$, so

  \[
  \alpha_{t_2}(f(s)) \subseteq f^\#(\alpha_{t_1}(s))
  \]

\[
\square
\]

Proof of Proposition 7

We can prove this proposition by structural induction on $t$.

- $t = K$. If $z = d$, then $s = \{\top\} \in \Gamma_K(d)$ holds that $\alpha_K(s) = d$. If $z = n$, then $s = [K] \in \Gamma_K(n)$ holds that $\alpha_K(s) = n$ whenever $[K]$ has at least two elements different from $\top$.

- $t = (t_1, \ldots, t_m)$. Let $z = (z_1, \ldots, z_m)$. By induction hypothesis on each $t_i$, then for each $i \in \{1, \ldots, m\}$ there exists $s_i \in \Gamma_{t_i}(z_i)$ such that $\alpha_{t_i}(s_i) = z_i$. So, $s = (s_1, \ldots, s_m)$ holds that $\alpha_t(s) = z$ by definition of $\alpha_t$. 

\( t = T \): If \( z = n \), then \( s = [T] \in \Gamma_t(n) \) holds that \( \alpha_t(s) = n \) whenever \([T]\) has at least two elements different from \( \bot \).

If \( z = d \) then \( s = \{ \bot \} \in \Gamma_t(d) \) holds that \( \alpha_t(s) = d \) trivially.

\( t = t_1 \rightarrow t_2 \). Let \( f^\# \in D_{2t_1} \); we are looking for \( f \in \Gamma_t(f^\#) \) such that \( \alpha_t(f) = f^\# \).

For each \( r \in A_{t_1} \), \( \alpha_{t_1}(r) \in D_{2t_1} \) and \( f^\#(\alpha_{t_1}(r)) \in D_{2t_2} \). By induction hypothesis on \( t_2 \), there exists \( s_r \in \Gamma_{t_2}(f^\#(\alpha_{t_1}(r))) \) such that \( \alpha_{t_2}(s_r) = f^\#(\alpha_{t_1}(r)) \).

Let us take \( f = \lambda r \in A_{t_1}, s_r \), where \( s_r \in \Gamma_{t_2}(f^\#(\alpha_{t_1}(r))) \) and \( \alpha_{t_2}(s_r) = f^\#(\alpha_{t_1}(r)) \) (we have just proved there exists one that holds that). Trivially \( f \in \Gamma_t(f^\#) \).

We have that

\[
\alpha_{t}(f) = \lambda z \in D_{2t_1}, \bigcup_{s_1, r \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)) = \lambda z \in D_{2t_1}, \bigcup_{s_1, r \in \Gamma_{t_1}(z)} \alpha_{t_2}(s_1, r)
\]

where \( s_1, r \in \Gamma_{t_2}(f^\#(\alpha_{t_1}(s_1))) \) and \( \alpha_{t_2}(s_1, r) = f^\#(\alpha_{t_1}(s_1)) \). We want to prove that given \( z \in D_{2t_1}, \bigcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(s_1, r) = f^\#(z) \), i.e. \( \bigcup_{s_1 \in \Gamma_{t_1}(z)} f^\#(\alpha_{t_1}(s_1)) = f^\#(z) \):

- \( (\subseteq) \). Each \( s_1 \in \Gamma_{t_1}(z) \) holds that \( \alpha_{t_1}(s_1) \subseteq z \) by Proposition 6, and by monotonicity of \( f^\# \) we have that \( f^\#(\alpha_{t_1}(s_1)) \subseteq f^\#(z) \). Consequently,

\[
\bigcup_{s_1 \in \Gamma_{t_1}(z)} f^\#(\alpha_{t_1}(s_1)) \subseteq f^\#(z)
\]

- \( (\supseteq) \). As \( z \in D_{2t_1} \), by induction hypothesis on \( t_1 \), there exists \( s_z \in \Gamma_{t_1}(z) \) such that \( \alpha_{t_1}(s_z) = z \). So

\[
f^\#(z) = f^\#(\alpha_{t_1}(s_z)) \subseteq \bigcup_{s_1 \in \Gamma_{t_1}(z)} f^\#(\alpha_{t_1}(s_1))
\]

\( \square \)

**Proof of Proposition 9**

We can prove this proposition by structural induction on \( t \). We also need some properties of the functions \( \phi_t \) and \( \mu_t \) that were proved in (Peña & Segura, 2001).

- \( t = K \). We have trivially that

\[
\alpha_K(s) \subseteq \mu_K(d) = d \iff det_K(s)
\]

- \( t = (t_1, \ldots, t_m) \). We have that

\[
\alpha_t((s_1, \ldots, s_m)) \subseteq \mu_t(d)
\]

\[
\iff \alpha_{t_i}(s_i) \subseteq \mu_{t_i}(d) \quad \forall i \in \{1..m\} \quad \{\text{by definition of } \alpha_t \text{ and } \mu_t\}
\]

\[
\iff det_{t_i}(s_i) \quad \forall i \in \{1..m\} \quad \{\text{by definition of } det_{t}\}
\]

- \( t = T \). This case is similar to the basic case \( t = K \).

- \( t = t_1 \rightarrow t_2 \).
Non-determinism Analyses

\[\forall z \in D_{2t_1} \quad \bigcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)) \subseteq \mu_{t_2}(\phi_1(z)) \quad (1)\]

We have to prove that \(\forall s \in A_{t_1}, \text{det}_{t_1}(s) \Rightarrow \text{det}_{t_2}(f(s))\). So, let \(s \in A_{t_1}\) such that \(\text{det}_{t_1}(s)\). By induction hypothesis on \(t_1\) then

\[\alpha_{t_1}(s) \subseteq \mu_{t_1}(d) \quad (2)\]

Additionally we know that for each type \(t\), \(\phi_t \cdot \mu_t = \text{id}_{\text{Basic}}\) (3), by Proposition 2(b) in (Peña & Segura, 2001).

In order to prove \(\text{det}_{t_2}(f(s))\), it is enough to prove that \(\alpha_{t_2}(f(s)) \subseteq \mu_{t_2}(d)\) by induction hypothesis on \(t_2\). Let us try this:

\[
\begin{align*}
\alpha_{t_2}(f(s)) & \subseteq \bigcup_{s_1 \in \Gamma_{t_1}(\alpha_{t_1}(s))} \alpha_{t_2}(f(s_1)) & \{\text{as } s \in \Gamma_{t_1}(\alpha_{t_1}(s))\} \\
& \subseteq \mu_{t_2}(\phi_1(\alpha_{t_1}(s))) & \{\text{by (1) when } z = \alpha_{t_1}(s)\} \\
& \subseteq \mu_{t_2}(\phi_1(\mu_{t_1}(d))) & \{\text{by (2) and monotonicity}\} \\
& = \mu_{t_2}(d) & \{\text{by (3)}\}
\end{align*}
\]

\(\Rightarrow\) If \(\text{det}_{t_1}(f)\) then

\[\forall s \in A_{t_1}, \text{det}_{t_1}(s) \Rightarrow \text{det}_{t_2}(f(s)) \quad (4)\]

We have to prove that

\[\forall z \in D_{2t_1} \quad \bigcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)) \subseteq \mu_{t_2}(\phi_1(z))\]

Let \(z \in D_{2t_1}\). We distinguish two cases.

\(- \ z \not\subseteq \mu_{t_1}(d)\). In this case \(\phi_{t_1}(z) = d\) (5) because \(\phi_t \cdot \mu_t = \text{id}_{\text{Basic}}\) by (3). We have that

\[
\begin{align*}
\Rightarrow s_1 \in \Gamma_{t_1}(z) & \Rightarrow \alpha_{t_1}(s_1) \subseteq z & \{\text{by Proposition 6}\} \\
& \Rightarrow \alpha_{t_1}(s_1) \subseteq \mu_{t_1}(d) & \{\text{as } z \subseteq \mu_{t_1}(d)\} \\
& \Rightarrow \text{det}_{t_2}(f(s_1)) & \{\text{i.h. on } t_1 \text{ and (4)}\} \\
& \Rightarrow \alpha_{t_2}(f(s_1)) \subseteq \mu_{t_2}(d) & \{\text{i.h. on } t_2\} \\
& \Rightarrow \alpha_{t_2}(f(s_1)) \subseteq \mu_{t_2}(\phi_1(z)) & \{\text{by (5)}\}
\end{align*}
\]

\(- \ z \not\subseteq \mu_{t_1}(d)\). By Proposition 3 in (Peña & Segura, 2001), \(\forall z \in D_{2t}, z \not\subseteq \mu_{t_1}(d) \Leftrightarrow \phi_t(z) = d\), so in this case \(\phi_t(z) = n\). We have to prove that \(\bigcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)) \subseteq \mu_{t_2}(n)\), which holds trivially as \(\mu_{t_1}(n)\) is the top element in \(D_{2t_1}\), by Proposition 2(d) in (Peña & Segura, 2001).

\[\Box\]

Proof of Proposition 10

This proposition can be proved by structural induction on \(e\). We need Propositions 6 and 9, and some properties satisfied by \(\phi_t\) and \(\mu_t\), proved in (Peña & Segura, 2001).

Additionally we need to prove that \(\alpha_t\) reflects the bottom element (Lemma 9 in (Segura & Peña, 2003)), and that the denotational semantics we have defined is monotone with respect to the environments (Lemma 10 in (Segura & Peña, 2003)). Both things can be proved by structural induction.
\[ e = k \vdash K. \] We have that
\[
\alpha_K([k] \rho) = \alpha_K([k, \bot]) \quad \{ \text{by definition of } [\cdot] \}
\]
\[
d = \{ \text{by definition of } \alpha_K \}
\]
\[ = [k]_2 \rho_2 \quad \{ \text{by definition of } [\cdot]_2 \} \]

\[ e = v :: t. \] In this case
\[
\alpha_t([v] \rho) = \alpha_t(\rho(v)) \quad \{ \text{by definition of } [\cdot] \}
\]
\[ \sqsubseteq \rho_2(v) \quad \{ \text{hypothesis of the proposition} \}
\]
\[ = [v]_2 \rho_2 \quad \{ \text{by definition of } [\cdot]_2 \} \]

\[ e = (x_1, \ldots, x_m) :: (t_1, \ldots, t_m). \]
\[
\alpha_{(t_1, \ldots, t_m)}([x_1, \ldots, x_m] \rho)
\]
\[ = (\alpha_{t_1}([x_1] \rho), \ldots, \alpha_{t_m}([x_m] \rho)) \quad \{ \text{by definition of } \alpha_\cdot \text{ and } [\cdot] \}
\]
\[ \sqsubseteq ([x_1]_2 \rho_2, \ldots, [x_m]_2 \rho_2) \quad \{ \text{i.h. on each } t_i \}
\]
\[ = ([x_1, \ldots, x_m]_2 \rho_2) \quad \{ \text{by definition of } [\cdot]_2 \} \]

\[ e = C \, x_1 \ldots \, x_m :: T. \] In this case
\[
\alpha_T(C \, x_1 \ldots \, x_m \rho)
\]
\[ = \alpha_T(C \, ([x_1] \rho) \ldots ([x_m] \rho))^* \quad \{ \text{by definition of } [\cdot] \}
\]
\[
= \begin{cases} 
  d & \text{if } det_T(C \, ([x_1] \rho) \ldots ([x_m] \rho))^* \\
  n & \text{otherwise}
\end{cases}
\]

We want to prove that \( \alpha_T(C \, x_1 \ldots \, x_m \rho) \sqsubseteq [C \, x_1 \ldots \, x_m]_2 \rho_2 \). We distinguish two cases:

If \( \alpha_T([C \, x_1 \ldots \, x_m] \rho) = d \) then it is trivial, as \( d \) is the bottom element in Basic.

If \( \alpha_T([C \, x_1 \ldots \, x_m] \rho) = n \), then \( \neg det_T(C \, ([x_1] \rho) \ldots ([x_m] \rho))^* \). In the set \( C \, ([x_1] \rho) \ldots ([x_m] \rho))^* \) there is just one constructor, so the only possibility for it to be non-deterministic, is that there exists \( i \in \{1..m\} \) such that \( \neg det_{t_i}(U[i_s] \, C \, s_1 \ldots s_m \in C \, ([x_1] \rho) \ldots ([x_m] \rho))^* \), i.e. such that \( \neg det_{t_i}(([x_i] \rho)} \). But, by Proposition 9, this implies that \( \alpha_{t_i}(([x_i] \rho) \not\sqsubseteq \mu_{t_i}(d) \). This implies that \( \phi_{t_i}(\alpha_{t_i}([x_i] \rho)) = n \) (1) (by Proposition 3 in (Peña & Segura, 2001)), so

\[
[C \, x_1 \ldots \, x_m]_2 \rho_2
\]
\[ = \bigcup^n_{j=1} \phi_{t_j}([x_j]_2 \rho_2) \quad \{ \text{by definition of } [\cdot]_2 \}
\]
\[ \sqsubseteq \bigcup^n_{j=1} \phi_{t_j}(\alpha_{t_j}([x_j] \rho)) \quad \{ \text{by i.h. on each } t_j \text{ and monotonicity} \}
\]
\[ = n \quad \{ \text{by (1)} \} \]

\[ e = \lambda v.e' :: t_1 \rightarrow t_2. \] On the one hand
\[
\alpha_{t_1 \rightarrow t_2}(\lambda v.e') \rho
\]
\[ = \alpha_{t_1 \rightarrow t_2}(\lambda s \in A_{t_1}. [e'] \rho[v \mapsto s]) \quad \{ \text{by definition of } [\cdot] \}
\]
\[ = \lambda z \in D_{t_1}. \bigcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_1}(e'[v \mapsto s_1]) \quad \{ \text{by definition of } \alpha_\cdot \}
\]

On the other hand
\[
[e]_2 \rho_2 = \lambda z \in D_{t_1}. [e']_2 \rho_2[v \mapsto z]
\]
Let $z \in D_{2t_1}$. We have to prove that

$$\bigcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{e_2}(\rho[v \mapsto s_1]) \subseteq [e']_2 \rho_2[v \mapsto z]$$

If $s_1 \in \Gamma_{t_1}(z)$ then $\alpha_{e_1}(s_1) \subseteq z$ by Proposition 6, so $\rho[v \mapsto s_1]$ and $\rho_2[v \mapsto z]$ satisfy the theorem hypothesis about the environments. We can then apply induction hypothesis on $e'$ and obtain

$$\alpha_{e_2}(\rho[v \mapsto s_1]) \subseteq [e']_2 \rho_2[v \mapsto z]$$

and immediately holds what we wanted.

- $e = \text{merge}_t :: [t] \rightarrow [t] \rightarrow [t]$. This case is trivial as $[\text{merge}_t]_2 \rho_2$ is the top element in the corresponding abstract domain.

- $e = \text{let } v = e_1 \text{ in } e_2 :: t$, where $e_1 :: t_1$ and $e_2 :: t$. Applying induction hypothesis on $e_1$ we have that $\alpha_{e_1}(\rho) \subseteq \rho_2$ so $\rho[v \mapsto [e_1] \rho]$ and $\rho_2[v \mapsto [e_1] \rho_2]$ hold the hypothesis theorem. Consequently:

$$\alpha_{e_2}(\rho) = \alpha_{e_2}(\rho_2[v \mapsto [e_1] \rho]) \quad \text{by definition of } \llbracket \cdot \rrbracket$$

$$\subseteq [e_2]_2 \rho_2[v \mapsto [e_1] \rho_2] \quad \text{by i.h. on } e_2$$

$$= [e_2]_2 \rho_2$$

- $e = \text{letrec } v_i = e_i \text{ in } e' :: t$, where $e_i :: t_i$ and $e' :: t$. By definition of $[\cdot]$ and $[\cdot]_2$, we have to prove that

$$\alpha_{e_i}([e']_2(\text{fix}(\lambda \rho. \rho[v_i \mapsto [e_i] \rho]))) \subseteq [e']_2(\text{fix}(\lambda \rho_2. \rho_2[v_i \mapsto [e_i]_2 \rho_2]))$$

We could apply induction hypothesis on $e'$ if the environments

$$A = \text{fix}(\lambda \rho. \rho[v_i \mapsto [e_i] \rho])$$

and

$$B = \text{fix}(\lambda \rho_2. \rho_2[v_i \mapsto [e_i]_2 \rho_2])$$

satisfied the hypothesis theorem, i.e. for each variable $v :: t_v$, $\alpha_{e_i}(A(v)) \subseteq B(v)$.

Both the concrete and abstract domains are pointed cpos, so

$$A = \bigcup_{n \in \mathbb{N}} (\lambda \rho. \rho[v_i \mapsto [e_i] \rho])^n(\rho_0)$$

and

$$B = \bigcup_{n \in \mathbb{N}} (\lambda \rho_2. \rho_2[v_i \mapsto [e_i]_2 \rho_2])^n(\rho_0)$$

where for each variable $v :: t_v$, $\rho_0(v) = \bot_{A_{t_v}}$ and $\rho_0(\alpha)(v) = \bot_{D_{2t_v}}$. Let us call $G = \lambda \rho. \rho[v \mapsto [e] \rho]$ and $F = \lambda \rho_2. \rho_2[v \mapsto [e]_2 \rho_2]$. We are going to prove that

$$\forall n \in \mathbb{N}. \forall v :: t_v. \alpha_{\epsilon v}(G^n(\rho_0)(v)) \subseteq F^n(\rho_0(\alpha))(v) \quad (2)$$

Then we will have that

$$\bigcup_{n \in \mathbb{N}} \alpha_{\epsilon v}(G^n(\rho_0)(v)) \subseteq \bigcup_{n \in \mathbb{N}} F^n(\rho_0(\alpha))(v)$$
As $\alpha_i$ is continuous and $G^n(\varrho_0)(v)$ is an ascending chain then
\[
\alpha_{tv}(\bigsqcup_{n \in \mathbb{N}} G^n(\varrho_0)(v)) \sqsubseteq \bigsqcup_{n \in \mathbb{N}} F^n(\varrho_2)(v)
\]
and we would have finished.

We prove (2) by induction on $n$. If $n = 0$, it is trivial as $\alpha_i(\bot_{A_k}) = \bot_{D_{2t}}$ by Lemma 9 in (Segura & Peña, 2003).

If $n > 0$, the induction hypothesis says that
\[
\forall v :: tv. \alpha_{tv}(G^n(\varrho_0)(v)) \sqsubseteq F^n(\varrho_2)(v) \tag{3}
\]
i.e. $G^n(\varrho_0)$ and $F^n(\varrho_2)$ hold the hypothesis theorem.

We have to prove that
\[
\forall v :: tv. \alpha_{tv}(G^{n+1}(\varrho_0)(v)) \sqsubseteq F^{n+1}(\varrho_2)(v)
\]
where $G^{n+1} = G \cdot G^n$ and $F^{n+1} = F \cdot F^n$.

Let $v :: tv$. We distinguish two cases. If $v \neq v_i \forall i$, then
\[
\alpha_{tv}(G^{n+1}(\varrho_0)(v)) = \alpha_{tv}(\varrho(v)) \sqsubseteq \varrho_2(v) = F^{n+1}(\varrho_2)(v)
\]
If there is any $v_i$ such that $v = v_i$, then
\[
\alpha_{tv}(G^{n+1}(\varrho_0)(v)) = \alpha_{tv}(\{e_i\} (G^n(\varrho_0))) = \square \{e_i\}_2 (F^n(\varrho_2)) \sqsubseteq F^{n+1}(\varrho_2)(v) \tag{by definition of $G$ and (3) and i.h. on $e_i$}
\]

- $e = \text{case } e_1 \text{ of } (v_1, \ldots, v_m) \rightarrow e_2 :: t$ where $e_1 :: (t_1, \ldots, t_m)$. By induction hypothesis on $e_1$ and definition of $\alpha_i$, the environments $\rho [v_i \mapsto \pi_i(\{e_i\} \rho)]$ and $\rho_2 [v_i \mapsto \pi_i(\{e_i\}_2 \rho_2)]$ hold the theorem hypothesis, so we can apply induction hypothesis on $e'$ and trivially obtain what we want.

- $e = \text{case } e' \text{ of } C_i \mapsto C_i[v \mapsto e''] :: t$, where $e' :: T$ and $e_i, e'' :: t$.

By definition
\[
[e] \rho = \begin{cases}
\bot_{A_k} & \text{if } e' \rho = \bot_{A_k} \\
\square \{e_i\}_k \rho [v_{kj} \mapsto s_{kj}]^{m_k} & \text{if } C_k s_{k1} \ldots s_{km} \in [e'] \rho \text{ otherwise}
\end{cases}
\]

So we distinguish two cases. If $[e'] \rho = \bot_{A_k}$, it is trivial as $\alpha_i(\bot_{A_k}) = \bot_{D_{2t}}$ by Lemma 9 in (Segura & Peña, 2003).

Otherwise, by induction hypothesis on $e'$ we have that $\alpha_T(\{e'\} \rho) \subseteq [e']_2 \rho_2$.

We distinguish again two cases. If $[e']_2 \rho_2 = n$ then it is trivial, as $[e']_2 \rho_2 = \mu_\eta(n)$ which is the top in $D_{2t}$ (by Proposition 2(d) in (Peña & Segura, 2001)).

If $[e']_2 \rho_2 = d$, then $\alpha_T(\{e'\} \rho) = d$, so $\det_T(\{e'\} \rho)$ by Proposition 9. This means that in $[e'] \rho$ there is at most a unique constructor $C_k$ and that for each $i \in \{1, \ldots, m_k\}$
\[
\det_{t_{si}}(\cup \{s_i \mid C_k s_{i1} \ldots s_{im} \in [e'] \rho\})
\]
which implies by Proposition 9 that
\[
\alpha_{t_{si}}(\cup \{s_i \mid C_k s_{i1} \ldots s_{im} \in [e'] \rho\}) \sqsubseteq \mu_{t_{si}}(d) \tag{4}
\]
This implies that

\[
\alpha(\{e_k\}_{1\leq i \leq n} \mid \rho \rightarrow s_k \rightarrow_{t} s_{k}^{m_k} \mid C_k \rightarrow_{t} s_{k}^{m_k} \in \{e\} \rho)
\]

\[\subseteq \alpha(\{e_k\}_{1\leq i \leq n} \mid \rho \rightarrow s_k \rightarrow_{t} s_{k}^{m_k} \mid C_k \rightarrow_{t} s_{k}^{m_k} \in \{e\} \rho)
\]

(by Lemma 10 in (Segura & Peña, 2003))

\[\subseteq \{e_k\}_{1\leq i \leq n} \rho_2[s_k \rightarrow \mu_{t_k}(d)]^{m_k}
\]

(by (4) and i.h. on \(e_k\))

\[\subseteq \{e_{i_1}\}_{1\leq i_1 \leq n} \rho_2[s_{i_1} \rightarrow \mu_{t_{i_1}}(d)]^{m_{i_1}}
\]

References
