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@sip.ucm.es,csegura@sip.ucm.es)

Proof of Proposition 4

This proposition can be proved by structural induction on e. Let $\mathcal{W}'_t : D_{2t} \rightarrow D_{2t}$ be a widening operator for each type t. All the cases but the recursive *let* expression can be easily proved by using the hypothesis over the environments, the induction hypothesis and the monotonicity properties of ϕ_t and μ_t, proved in (Peña & Segura, 2001). So, here we only look at the recursive *let* expression.

Let $e = \textbf{let rec}\ \overline{\{v_i = e_i\}}\ \textbf{in}\ e' :: t$, where $e' :: t$, and each v_i and e_i have type t_i. On the one hand

$$[\![e]\!]_2\ \rho_2 = [\![e']\!]_2\ (\bigsqcup_{n \in \mathbb{N}} (\lambda \rho'_2.\rho_2\ \overline{[v_i \rightarrow [\![e_i]\!]_2\ \rho'_2]})^n(\rho_{02}))$$

where ρ_{02} is the initial environment where each variable $y :: t_y$ has $\bot_{t_y}$ as abstract value (that is, the infimum of the corresponding domain). Let F be the function between environments $\lambda \rho'_2.\rho_2\ \overline{[v_i \rightarrow [\![e_i]\!]_2\ \rho'_2]}$. Let ρ_2^{fix} be $\bigsqcup_{n \in \mathbb{N}} F^n(\rho_{02})$.

On the other hand

$$[\![e]\!]_3^{\mathcal{W}'} \rho_t = [\![e']\!]_3^{\mathcal{W}'} (\bigsqcup_{n \in \mathbb{N}} (\lambda \rho'_3.\rho_3\ \overline{[v_i \rightarrow \mathcal{W}'_{t_i}([\![e_i]\!]_3^{\mathcal{W}'} \rho'_3)]})^n(\rho_{03}))$$

where ρ_{03} is the initial environment where each variable $y :: t_y$ has $\bot_{t_y}$ as abstract value (that is, the infimum of the corresponding domain). Let G be the function between environments $\lambda \rho'_3.\rho_3\ \overline{[v_i \rightarrow \mathcal{W}'_{t_i}([\![e_i]\!]_3^{\mathcal{W}'} \rho'_3)]}$. Let ρ_3^{fix} be $\bigsqcup_{n \in \mathbb{N}} G^n(\rho_{03})$.

If we proved that for each variable $y :: t_y$, $\rho_2^{fix}(y) \sqsubseteq \rho_3^{fix}(y)$, then by induction hypothesis we would have that

$$[\![e']\!]_2\ \rho_2^{fix} \sqsubseteq [\![e']\!]_3^{\mathcal{W}'} \rho_3^{fix}$$

which is what we want to prove. Let us see that for each $n \geq 0$, the following holds:

$$\forall y :: t_y.(F^n(\rho_{02}))(y) \sqsubseteq (G^n(\rho_{03}))(y)$$

If this were true then

$$\forall y :: t_y.(\bigsqcup_{n \in \mathbb{N}} F^n(\rho_{02}))(y) \sqsubseteq (\bigsqcup_{n \in \mathbb{N}} G^n(\rho_{03}))(y)$$

and we would be done. It can be proved by induction on n:

- $n = 0$. This is a trivial case as $F^0(\rho_{02}) = \rho_{02}$, $G^0(\rho_{03}) = \rho_{03}$, which are equal.

- $n = m+1$. Then

$$\begin{array}{rcl} F^{m+1}(\rho_{02}) & = & F(F^m(\rho_{02})) \\ & = & \rho_2\ \overline{[v_i \to [\![e_i]\!]_2\ (F^m(\rho_{02}))]} \quad \{\text{by definition of } F\} \end{array}$$

and

$$\begin{array}{rcl} G^{m+1}(\rho_{03}) & = & G(G^m(\rho_{03})) \\ & = & \rho_3\ \overline{[v_i \to \mathcal{W}'_{t_i}([\![e_i]\!]_3^{\mathcal{W}'}(G^m(\rho_{03})))]} \quad \{\text{by definition of } G\} \end{array}$$

Let $y :: t_y$. We want to prove that $(F^{m+1}(\rho_{02}))(y) \sqsubseteq (G^{m+1}(\rho_{03}))(y)$. We distinguish two cases. If y is not any of the v_i, then it holds by the hypothesis over the environments ρ_2 and ρ_3. If it is one of the v_i, then we have to prove that

$$[\![e_i]\!]_2\ (F^m(\rho_{02})) \sqsubseteq \mathcal{W}'_{t_i}([\![e_i]\!]_3^{\mathcal{W}'}(G^m(\rho_{03})))$$

This holds by induction hypothesis and by the hypothesis on $\mathcal{W}'_t$:

$$[\![e_i]\!]_2\ (F^m(\rho_{02})) \sqsubseteq [\![e_i]\!]_3^{\mathcal{W}'}(G^m(\rho_{03})) \sqsubseteq \mathcal{W}'_{t_i}([\![e_i]\!]_3^{\mathcal{W}'}(G^m(\rho_{03})))$$

□

Proof of Proposition 5
This proof is very similar to the previous one. The same steps can be followed in the recursive *let* expression, being now

$$F = \lambda\rho'_3.\rho_3\ \overline{[v_i \to \mathcal{W}'_{t_i}([\![e_i]\!]_3^{\mathcal{W}'}\ \rho'_3)]})^n(\rho_{03}))$$

and

$$G = \lambda\rho''_3.\rho_3\ \overline{[v_i \to \mathcal{W}''_{t_i}([\![e_i]\!]_3^{\mathcal{W}''}\ \rho''_3)]})^n(\rho_{03}))$$

The same induction on n is done, and at the end we have to prove that

$$\mathcal{W}'_{t_i}([\![e_i]\!]_3^{\mathcal{W}'}(F^m(\rho_{02}))) \sqsubseteq \mathcal{W}''_{t_i}([\![e_i]\!]_3^{\mathcal{W}''}(G^m(\rho_{03})))$$

which is true by induction hypothesis, $\mathcal{W}'_t \sqsubseteq \mathcal{W}''_t$ and monotonicity of $\mathcal{W}''_t$ (proved in (Peña & Segura, 2001)):

$$\begin{array}{rcl} \mathcal{W}'_{t_i}([\![e_i]\!]_3^{\mathcal{W}'}(F^m(\rho_{02}))) & \sqsubseteq & \mathcal{W}''_{t_i}([\![e_i]\!]_3^{\mathcal{W}'}(F^m(\rho_{02}))) \\ & \sqsubseteq & \mathcal{W}''_{t_i}([\![e_i]\!]_3^{\mathcal{W}''}(G^m(\rho_{03}))) \end{array}$$

□

Proof of Proposition 6
This proposition can be proved by structural induction on t.

- $t = K$.
  - (⇒). If $z = n$, then trivially $\alpha_t(s) \sqsubseteq n$, as n is the top of *Basic*.
    If $z = d$, then if $s \in \Gamma_K(d)$, by definition of Γ_t, we have that $unit(s)$ is true, which implies that $\alpha_K(s) = d$ by definition of α_t.
  - (⇐). If $z = d$, $\alpha_K(s) \sqsubseteq d$ implies $unit(s)$, so $s \in \Gamma_K(d)$ by definition of Γ_t.
    If $z = n$, then trivially $s \in \Gamma_K(n) = \mathcal{P}(A_K)$.

- $t = (t_1, \ldots, t_m)$.

$$\begin{array}{ll} (s_1, \ldots, s_m) \in \Gamma_t(z_1, \ldots, z_m) & \\ \quad \Leftrightarrow \forall i \in \{1..m\}.\alpha_{t_i}(s_i) \sqsubseteq z_i & \{\text{by definition of } \Gamma_t\} \\ \quad \Leftrightarrow \alpha_t(s_1, \ldots, s_n) \sqsubseteq (z_1, \ldots, z_m) & \{\text{by definition of } \alpha_t\} \end{array}$$

- $t = T$.

— ($\Rightarrow$). If $z = n$, then trivially $\alpha_t(s) \sqsubseteq n$, as n is the top of *Basic*.
If $z = d$, then if $s \in \Gamma_T(d)$, by definition of Γ_t, we have that $det_T(s)$ which implies that $\alpha_T(s) = d$ by definition of α_t.

— ($\Leftarrow$). If $z = d$, $\alpha_T(s) \sqsubseteq d$ implies $det_T(s)$, so $s \in \Gamma_T(d)$ by definition of Γ_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,

$$\forall s \in A_{t_1}.\alpha_{t_2}(f(s)) \sqsubseteq f^\#(\alpha_{t_1}(s)) \quad (1)$$

Let $z \in D_{2t}$. We have to prove that $\alpha_t(f)(z) \sqsubseteq f^\#(z)$. 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) $\alpha_{t_2}(f(s_1)) \sqsubseteq f^\#(\alpha_{t_1}(s_1))$. So

$$\bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)) \sqsubseteq \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} f^\#(\alpha_{t_1}(s_1)) \quad (2)$$

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

— ($\Leftarrow$). If $\alpha_t(f) \sqsubseteq f^\#$, then by definition of α_t,

$$\forall z \in D_{2t_1} \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)) \sqsubseteq f^\#(z) \quad (3)$$

Let $s \in A_{t_1}$. We have to prove that $\alpha_{t_2}(f(s)) \sqsubseteq f^\#(\alpha_{t_1}(s))$.
As $\alpha_{t_1}(s) \in D_{2t_1}$, by (3) we have that $\bigsqcup_{s_1 \in \Gamma_{t_1}(\alpha_{t_1}(s))} \alpha_{t_2}(f(s_1)) \sqsubseteq f^\#(\alpha_{t_1}(s))$.
By induction hypothesis, trivially $s \in \Gamma_{t_1}(\alpha_{t_1}(s))$, so

$$\alpha_{t_2}(f(s)) \sqsubseteq \bigsqcup_{s_1 \in \Gamma_{t_1}(\alpha_{t_1}(s))} \alpha_{t_2}(f(s_1)) \sqsubseteq f^\#(\alpha_{t_1}(s))$$

□

Proof of Proposition 7
We can prove this proposition by structural induction on t.

- $t = K$. If $z = d$, then $s = \{\perp\} \in \Gamma_K(d)$ 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 $\perp$.
- $t = (t_1, \ldots, t_m)$. Let $z = (z_1, \ldots, z_m)$. By induction hypothesis on each t_i, then for each $i \in \{1..m\}$ 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 α_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.
- $t = t_1 \to t_2$. Let $f^\# \in D_{2t}$; 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

$$\alpha_t(f) = \lambda z \in D_{2t_1}. \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)) = \lambda z \in D_{2t_1}. \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(s_{1r})$$

  where $s_{1r} \in \Gamma_{t_2}(f^\#(\alpha_{t_1}(s_1)))$ and $\alpha_{t_2}(s_{1r}) = f^\#(\alpha_{t_1}(s_1))$. We want to prove that given $z \in D_{2t_1}$, $\bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(s_{1r}) = f^\#(z)$, i.e. $\bigsqcup_{s_1 \in \Gamma_{t_1}(z)} f^\#(\alpha_{t_1}(s_1)) = f^\#(z)$:

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

$$\bigsqcup_{s_1 \in \Gamma_{t_1}(z)} f^\#(\alpha_{t_1}(s_1)) \sqsubseteq f^\#(z)$$

  — ($\sqsupseteq$). As $z \in D_{2t_1}$, by induction hypoythesis on t_1, there exists $s_z \in \Gamma_{t_1}(z)$ such that $\alpha_{t_1}(s_z) = z$. So

$$f^\#(z) = f^\#(\alpha_{t_1}(s_z)) \sqsubseteq \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} f^\#(\alpha_{t_1}(s_1))$$

$\square$

Proof of Proposition 9

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

- $t = K$. We have trivially that

$$\alpha_K(s) \sqsubseteq \mu_K(d) = d \Leftrightarrow det_K(s)$$

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

$$\begin{array}{lll} \multicolumn{3}{l}{\alpha_t((s_1, \ldots, s_m)) \sqsubseteq \mu_t(d)} \\ & \Leftrightarrow \alpha_{t_i}(s_i) \sqsubseteq \mu_{t_i}(d) \;\; \forall i \in \{1..m\} & \{\text{by definition of } \alpha_t \text{ and } \mu_t\} \\ & \Leftrightarrow det_{t_i}(s_i) \;\; \forall i \in \{1..m\} & \{\text{by induction hypothesis on } t_i\} \\ & \Leftrightarrow det_t((s_1, \ldots, s_m)) & \{\text{by definition of } det_t\} \end{array}$$

- $t = T$. This case is similar to the basic case $t = K$.
- $t = t_1 \to t_2$.

— $(\Rightarrow)$.If $\alpha_t(f) \sqsubseteq \mu_t(d)$, then

$$\forall z \in D_{2t_1}. \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)) \sqsubseteq \mu_{t_2}(\phi_{t_1}(z)) \quad (1)$$

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

$$\alpha_{t_1}(s) \sqsubseteq \mu_{t_1}(d) \quad (2)$$

Additionally we know that for each type t, $\phi_t \cdot \mu_t = id_{Basic}$ (3), by Proposition 2(b) in (Peña & Segura, 2001).
In order to prove $det_{t_2}(f(s))$, it is enough to prove that $\alpha_{t_2}(f(s)) \sqsubseteq \mu_{t_2}(d)$ by induction hypothesis on t_2. Let us try this:

$$\begin{array}{lll} \alpha_{t_2}(f(s)) & \sqsubseteq \bigsqcup_{s_1 \in \Gamma_{t_1}(\alpha_{t_1}(s))} \alpha_{t_2}(f(s_1)) & \{\text{as } s \in \Gamma_{t_1}(\alpha_{t_1}(s))\} \\ & \sqsubseteq \mu_{t_2}(\phi_{t_1}(\alpha_{t_1}(s))) & \{\text{by (1) when } z = \alpha_{t_1}(s)\} \\ & \sqsubseteq \mu_{t_2}(\phi_{t_1}(\mu_{t_1}(d))) & \{\text{by (2) and monotonicity}\} \\ & = \mu_{t_2}(d) & \{\text{by (3) }\} \end{array}$$

— $(\Leftarrow)$. If $det_t(f)$ then

$$\forall s \in A_{t_1}.det_{t_1}(s) \Rightarrow det_{t_2}(f(s)) \quad (4)$$

We have to prove that

$$\forall z \in D_{2t_1}. \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)) \sqsubseteq \mu_{t_2}(\phi_{t_1}(z))$$

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

- $z \sqsubseteq \mu_{t_1}(d)$. In this case $\phi_{t_1}(z) = d$ (5) because $\phi_t \cdot \mu_t = id_{Basic}$ by (3). We have that

$$\begin{array}{lll} s_1 \in \Gamma_{t_1}(z) & \Rightarrow \alpha_{t_1}(s_1) \sqsubseteq z & \{\text{by Proposition 6}\} \\ & \Rightarrow \alpha_{t_1}(s_1) \sqsubseteq \mu_{t_1}(d) & \{\text{as } z \sqsubseteq \mu_{t_1}(d)\} \\ & \Rightarrow det_{t_2}(f(s_1)) & \{\text{by i.h. on } t_1 \text{ and } (4)\} \\ & \Rightarrow \alpha_{t_2}(f(s_1)) \sqsubseteq \mu_{t_2}(d) & \{\text{by i.h. on } t_2\} \\ & \Rightarrow \alpha_{t_2}(f(s_1)) \sqsubseteq \mu_{t_2}(\phi_{t_1}(z)) & \{\text{by (5)}\} \end{array}$$

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

□

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 ϕ_t and μ_t, proved in (Peña & Segura, 2001). Additionally we need to prove that α_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.

- $e = k :: K$. We have that

$$\begin{array}{lll} \alpha_K([\![k]\!]\ \rho) & = \alpha_K(\{k,\bot\}) & \{\text{by definition of } [\![\cdot]\!]\} \\ & = d & \{\text{by definition of } \alpha_K\} \\ & = [\![k]\!]_2\ \rho_2 & \{\text{by definition of } [\![\cdot]\!]_2\} \end{array}$$

- $e = v :: t$. In this case

$$\begin{array}{lll} \alpha_t([\![v]\!]\ \rho) & = \alpha_t(\rho(v)) & \{\text{by definition of } [\![\cdot]\!]\} \\ & \sqsubseteq \rho_2(v) & \{\text{hypothesis of the proposition}\} \\ & = [\![v]\!]_2\ \rho_2 & \{\text{by definition of } [\![\cdot]\!]_2\} \end{array}$$

- $e = (x_1, \ldots, x_m) :: (t_1, \ldots, t_m)$.

$$\begin{array}{ll} \alpha_{(t_1,\ldots,t_m)}([\![(x_1,\ldots,x_m)]\!]\ \rho) & \\ \quad = (\alpha_{t_1}([\![x_1]\!]\ \rho), \ldots, \alpha_{t_m}([\![x_m]\!]\ \rho)) & \{\text{by definition of } \ \alpha_t \text{ and } [\![\cdot]\!]\} \\ \quad \sqsubseteq ([\![x_1]\!]_2\ \rho_2, \ldots, [\![x_m]\!]_2\ \rho_2) & \{\text{by i.h. on each } t_i\} \\ \quad = [\![(x_1,\ldots,x_m)]\!]_2\ \rho_2 & \{\text{by definition of } [\![\cdot]\!]_2\} \end{array}$$

- $e = C\ x_1 \ldots x_m :: T$. In this case

$$\begin{array}{ll} \alpha_T([\![C\ x_1 \ldots x_m]\!]\ \rho) & \\ \quad = \alpha_T(\{C\ ([\![x_1]\!]\ \rho) \ldots ([\![x_m]\!]\ \rho)\}^*) & \{\text{by definition of } [\![\cdot]\!]\} \\ \quad = \left\{ \begin{array}{ll} d & \text{if } det_T(\{C\ ([\![x_1]\!]\ \rho) \ldots ([\![x_m]\!]\ \rho)\}^*) \\ n & \text{otherwise} \end{array} \right. & \end{array}$$

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 $\neg det_{t_i}(\sqcup\{s_i \mid C\ s_1 \ldots s_m \in \{C\ ([\![x_1]\!]\ \rho) \ldots ([\![x_m]\!]\ \rho)\}^*\})$, 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

$$\begin{array}{ll} [\![C\ x_1 \ldots x_m]\!]_2\ \rho_2 & \\ \quad = \bigsqcup_{j=1}^{m} \phi_{t_j}([\![x_j]\!]_2\ \rho_2) & \{\text{by definition of } [\![\cdot]\!]_2\} \\ \quad \sqsupseteq \bigsqcup_{j=1}^{m} \phi_{t_j}(\alpha_{t_j}([\![x_j]\!]\ \rho)) & \{\text{by i.h. on each } t_j \text{ and monotonicity}\} \\ \quad = n & \{\text{by (1)}\} \end{array}$$

- $e = \lambda v.e' :: t_1 \to t_2$. On the one hand

$$\begin{array}{ll} \alpha_{t_1 \to t_2}([\![\lambda v.e']\!]\ \rho) & \\ \quad = \alpha_{t_1 \mapsto t_2}(\lambda s \in A_{t_1}.[\![e']\!]\ \rho[v \mapsto s]) & \{\text{by definition of } [\![\cdot]\!]\} \\ \quad = \lambda z \in D_{2 t_1}.\bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}([\![e']\!]\ \rho[v \mapsto s_1]) & \{\text{by definition of } \alpha_t\} \end{array}$$

On the other hand

$$[\![e]\!]_2\ \rho_2 = \lambda z \in D_{2 t_1}.[\![e']\!]_2\ \rho_2[v \mapsto z]$$

Let $z \in D_{2t_1}$. We have to prove that

$$\bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(\llbracket e' \rrbracket\ \rho[v \mapsto s_1]) \sqsubseteq \llbracket e' \rrbracket_2\ \rho_2[v \mapsto z]$$

If $s_1 \in \Gamma_{t_1}(z)$ then $\alpha_{t_1}(s_1) \sqsubseteq z$ 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

$$\alpha_{t_2}(\llbracket e' \rrbracket\ \rho[v \mapsto s_1]) \sqsubseteq \llbracket e' \rrbracket_2\ \rho_2[v \mapsto z]$$

and immediately holds what we wanted.

- $e = merge_t :: [t] \to [t] \to [t]$. This case is trivial as $\llbracket merge_t \rrbracket_2\ \rho_2$ is the top element in the corresponding abstract domain.
- $e =$ **let** $v = e_1$ **in** $e_2 :: t$, where $e_1 :: t_1$ and $e_2 :: t$. Applying induction hypothesis on e_1 we have that $\alpha_{t_1}(\llbracket e_1 \rrbracket\ \rho) \sqsubseteq \llbracket e_1 \rrbracket_2\ \rho_2$, so $\rho[v \mapsto \llbracket e_1 \rrbracket\ \rho]$ and $\rho_2[v \mapsto \llbracket e_1 \rrbracket_2\ \rho_2]$ hold the hypothesis theorem. Consequently:

$$\begin{array}{ll} \alpha_t(\llbracket e \rrbracket\ \rho) & = \alpha_t(\llbracket e_2 \rrbracket\ \rho[v \mapsto \llbracket e_1 \rrbracket\ \rho]) \quad \{\text{by definition of } \llbracket \cdot \rrbracket\} \\ & \sqsubseteq \llbracket e_2 \rrbracket_2\ \rho_2[v \mapsto \llbracket e_1 \rrbracket_2\ \rho_2] \quad \{\text{by i.h. on } e_2\} \\ & = \llbracket e \rrbracket_2\ \rho_2 \end{array}$$

- $e =$ **letrec** $\overline{v_i = e_i}$ **in** $e' :: t$, where $e_i :: t_i$ and $e' :: t$. By definition of $\llbracket \cdot \rrbracket$ and $\llbracket \cdot \rrbracket_2$ we have to prove that

$$\alpha_t(\llbracket e' \rrbracket\ (\mathit{fix}\ (\lambda\rho'.\rho\ \overline{[v_i \mapsto \llbracket e_i \rrbracket\ \rho']}))) \sqsubseteq \llbracket e' \rrbracket_2\ (\mathit{fix}(\lambda\rho'_2.\rho_2\ \overline{[v_i \mapsto \llbracket e_i \rrbracket_2\ \rho'_2]}))$$

We could apply induction hypothesis on e' if the environmets

$$A = \mathit{fix}\ (\lambda\rho'.\rho\ \overline{[v_i \mapsto \llbracket e_i \rrbracket\ \rho']})$$

and

$$B = \mathit{fix}(\lambda\rho'_2.\rho_2\ \overline{[v_i \mapsto \llbracket e_i \rrbracket_2\ \rho'_2]})$$

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

Both the concrete and abstract domains are pointed cpos, so

$$A = \bigsqcup_{n \in \mathbb{N}} (\lambda\rho'.\rho\ \overline{[v_i \mapsto \llbracket e_i \rrbracket\ \rho']})^n(\rho_0)$$

and

$$B = \bigsqcup_{n \in \mathbb{N}} (\lambda\rho'_2.\rho_2\ \overline{[v_i \mapsto \llbracket e_i \rrbracket_2\ \rho'_2]})^n(\rho_{02})$$

where for each variable $v :: tv$, $\rho_0(v) = \bot_{A_{tv}}$ and $\rho_{02}(v) = \bot_{D_{2tv}}$. Let us call $G = \lambda\rho'.\rho\ \overline{[v_i \mapsto \llbracket e_i \rrbracket\ \rho']}$ and $F = \lambda\rho'_2.\rho_2\ \overline{[v_i \mapsto \llbracket e_i \rrbracket_2\ \rho'_2]}$. We are going to prove that

$$\forall n \in \mathbb{N}. \forall v :: tv. \alpha_{tv}(G^n(\rho_0)(v)) \sqsubseteq F^n(\rho_{02})(v) \quad (2)$$

Then we will have that

$$\bigsqcup_{n \in \mathbb{N}} \alpha_{tv}(G^n(\rho_0)(v)) \sqsubseteq \bigsqcup_{n \in \mathbb{N}} F^n(\rho_{02})(v)$$

As α_t is continuous and $G^n(\rho_0)(v)$ is an ascending chain then

$$\alpha_{tv}(\bigsqcup_{n\in\mathbb{N}} G^n(\rho_0)(v)) \sqsubseteq \bigsqcup_{n\in\mathbb{N}} F^n(\rho_{02})(v)$$

and we would have finished.
We prove (2) by induction on n. If $n=0$, it is trivial as $\alpha_t(\bot_{A_t}) = \bot_{D_{2t}}$ by Lemma 9 in (Segura & Peña, 2003).
If $n>0$, the induction hypothesis says that

$$\forall v :: tv.\alpha_{tv}(G^n(\rho_0)(v)) \sqsubseteq F^n(\rho_{02})(v) \quad (3)$$

i.e. $G^n(\rho_0)$ and $F^n(\rho_{02})$ hold the hypothesis theorem.
We have to prove that

$$\forall v :: tv.\alpha_{tv}(G^{n+1}(\rho_0)(v)) \sqsubseteq F^{n+1}(\rho_{02})(v)$$

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

$$\alpha_{tv}(G^{n+1}(\rho_0)(v)) = \alpha_{tv}(\rho(v)) \sqsubseteq \rho_2(v) = F^{n+1}(\rho_{02}(v))$$

If there is any v_i such that $v = v_i$, then

$$\begin{array}{lll} \alpha_{tv}(G^{n+1}(\rho_0)(v)) & = \alpha_{tv}([\![e_i]\!]\ (G^n(\rho_0))) & \{\text{by definition of } G\} \\ & \sqsubseteq [\![e_i]\!]_2\ (F^n(\rho_{02})) & \{\text{by (3) and i.h. on } e_i\} \\ & = F^{n+1}(\rho_{02})(v) & \{\text{by definition of } F\} \end{array}$$

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

$$[\![e]\!]\ \rho = \left\{ \begin{array}{l} \bot_{A_t}\ \text{if}\ [\![e']\!]\ \rho = \bot_{A_T} \\ \bigsqcup_{A_t}\{[\![e_k]\!]\ \rho\overline{[v_{kj} \mapsto s_{kj}]}^{m_k} \mid C_k\ \overline{s_{kj}}^{m_k} \in [\![e]\!]\ \rho\}\ \text{otherwise} \end{array} \right.$$

So we distinguish two cases. If $[\![e']\!]\ \rho = \bot_{A_T}$, it is trivial as $\alpha_t(\bot_{A_t}) = \bot_{D_{2t}}$ by Lemma 9 in (Segura & Peña, 2003).
Otherwise, by induction hypothesis on e' we have that $\alpha_T([\![e']\!]\ \rho) \sqsubseteq [\![e']\!]_2\ \rho_2$. We distinguish again two cases. If $[\![e']\!]_2\ \rho_2 = n$ then it is trivial, as $[\![e]\!]_2\ \rho_2 = \mu_t(n)$ 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 $i \in \{1..m_k\}$

$$det_{t_{ki}}(\sqcup\{s_i \mid C_k\ s_1 \ldots s_{m_k} \in [\![e']\!]\ \rho)$$

which implies by Proposition 9 that

$$\alpha_{t_{ki}}(\sqcup\{s_i \mid C_k\ s_1 \ldots s_{m_k} \in [\![e']\!]\ \rho) \sqsubseteq \mu_{t_{ki}}(d) \quad (4)$$

This implies that

$$
\begin{array}{l}
\alpha_t(\bigsqcup_{A_t}\{[\![e_k]\!]\ \rho\overline{[v_{kj} \mapsto s_{kj}]}^{m_k} \mid C_k\ \overline{s_{kj}}^{m_k} \in [\![e']\!]\ \rho\} \\
\sqsubseteq \alpha_t([\![e_k]\!]\ \rho\overline{[v_{kj} \mapsto \bigsqcup s_{kj}] \mid C_k\ \overline{s_{kj}}^{m_k} \in [\![e']\!]\ \rho}^{m_k}) \\
\quad \{\text{by Lemma 10 in (Segura \& Peña, 2003)}\} \\
\sqsubseteq [\![e_k]\!]_2\ \rho_2\overline{[v_{kj} \mapsto \mu_{t_{kj}}(d)]}^{m_k} \\
\quad \{\text{by (4) and i.h. on } e_k\} \\
\sqsubseteq \bigsqcup\limits_i [\![e_i]\!]_2\ \rho_2\overline{[v_{ij} \mapsto \mu_{t_{ij}}(d)]}^{m_i}
\end{array}
$$

□

References

Peña, R., & Segura, C. (2001). *Three Non-determinism Analyses in a Parallel-Functional Language*. Technical Report 117-01, Dep. Sistemas Informáticos y Programación, Universidad Complutense de Madrid, Spain. (http://dalila.sip.ucm.es/miembros/clara/publications.html).

Segura, C., & Peña, R. (2003). *Correctness of Non-determinism Analyses in a Parallel-Functional Language*. Technical Report 131-03, Dep. Sistemas Informáticos y Programación, Universidad Complutense de Madrid, Spain. (http://dalila.sip.ucm.es/miembros/clara/publications.html).