A Posteriori Environment Analysis via Pushdown ΔCFA Technical Report

Kimball Germane   Matthew Might
University of Utah

$$\begin{aligned}
\bar{\varsigma} \in \overline{State} &= \overline{Eval} + \overline{Apply} \\
\overline{\text{E}} \in \overline{Eval} &= Call \times BEnv \times \overline{VEnv} \times \overline{Log} \times Time \\
\overline{\text{A}} \in \overline{Apply} &= \overline{Proc} \times \overline{D}^{*} \times \overline{VEnv} \times \overline{Log} \times Time \\
\overline{ve} \in \overline{VEnv} &= Var \times Time \rightharpoonup \overline{D} \\
\delta \in \overline{Log} &= Time \rightharpoonup F \\
\overline{d}, \overline{c} \in \overline{D} &= \overline{Proc} \\
\overline{proc} \in \overline{Proc} &= \overline{Clos} + \{halt\} \\
\overline{clos} \in \overline{Clos} &= Lam \times BEnv \times Time
\end{aligned}$$

Figure 1. Log state space

$\overline{Eval}$

$$(\ldots, \delta, t) \Rightarrow_{UE} (\ldots, \delta', t')$$

$$\begin{aligned}
p_\Delta &= \lfloor \delta(t'') \rfloor^{-1} \\
\delta' &= (\lambda t.\delta(t) + p_\Delta)[t' \mapsto \epsilon] \\
\overline{c} &= (L(\gamma), \beta, t'')
\end{aligned}$$

$\overline{Apply}$

$$(\ldots, \delta, t) \Rightarrow_{UA} (\ldots, \delta', t')$$

$$\begin{aligned}
p_\Delta &= \langle^{\psi}_{t'}| \\
\delta' &= (\lambda t.\delta(t) + p_\Delta)[t' \mapsto \epsilon] \\
\overline{proc} &= (L(\psi), \beta, t'')
\end{aligned}$$

$$\begin{aligned}
\overline{\mathcal{A}}(x, \beta, \overline{ve}, t) &= \overline{ve}(x, \beta(x)) \\
\overline{\mathcal{A}}(lam, \beta, \overline{ve}, t) &= (lam, \beta, t)
\end{aligned}$$

$$\overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) = (\ldots, \emptyset_\delta[t_0 \mapsto \epsilon], t_0)$$

Figure 2. Log Semantics

1. Introduction

This brief technical report contains theorems of correctness for the approach described in "A Posteriori Environment Analysis via Pushdown ΔCFA". Correctness is grounded in the *log semantics* of ΔCFA which we now present.

2. Log Semantics

The log semantics augments the the standard semantics in two ways: First, a closure is the triple (lam, β, t) instead of the pair (lam, β) where t is the timestamp of its birth. Second, each state acquires a log δ component, a map from times to delta frame strings. The effect of these additions can be seen in the log state space, presented in Figure 1: the $\overline{Log}$ domain was added and each other barred domain was altered to accommodate them. The log machine relation $\Rightarrow$ augments the transitions of the standard semantics as seen in Figure 2.

The bulk of the work of the log semantics is in keeping the log up-to-date, which requires calculating the delta frame string on each transition and recording it in the log. For $\overline{Apply}$–$\overline{Eval}$ transitions, the delta frame string is merely the single frame push $\langle^{\psi}_{t'}|$. For $\overline{Eval}$–$\overline{Apply}$ transitions, the birth time of the continuation $\overline{c}$ is used to determine which frames to pop. (The net operation ensures that the frames of tail calls, which pass their continuations unmodified, are popped only once.)

$\overline{\mathcal{A}}$ alters $\mathcal{A}$ to take an extra parameter, the timestamp t of the transition source state.

3. Delta Frame String Recovery

The delta frame string of an $\overline{Eval}$–$\overline{Apply}$ step is derived from the delta frame string since the birth of the call's continuation. The log semantics obtains this birth time by consulting the closure's timestamp. However, we can obtain the equivalent *birth state* from the path's decomposition.

3.1 Continuation Birth Time Recovery

Given a path $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^{+} \overline{\text{E}}$ for which we want the birth state $\overline{\text{E}_{birth}}$ of $\overline{\text{E}}$'s continuation $\overline{c}$, we define *btime* over $\bar{P}$ to produce $\bar{P}_{birth} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^{+} \overline{\text{E}_{birth}}$.

Definition 1 (Continuation Birth Time)**.** *If* $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^{+} \overline{\text{E}}$*, then* $btime(\bar{P})$ *is*

1. $\overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^{+} \overline{\text{EI}}$ *if* $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^{+} \overline{\text{EI}}$*;*
2. $\overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^{+} \overline{\text{UEI}}$ *if* $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^{+} \overline{\text{UEI}} \Rightarrow \overline{\text{UA}} \Rightarrow^{*} \overline{\text{EE}}$ *where* $\overline{\text{UA}} \in CE^{*}(\overline{\text{EE}})$*; and*
3. $\overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^{0} \overline{\text{UA}}$ *if* $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^{0} \overline{\text{UA}} \Rightarrow^{+} \overline{\text{EE}}$ *where* $\overline{\text{UA}} \in CE^{*}(\overline{\text{EE}})$.

Case 1 reflects that an $\overline{EvalInner}$ state has a λ-term $clam$ for its continuation expression meaning that its continuation is born in that state, at that time. Cases 2 and 3 reflect that an $\overline{EvalExit}$ state has a reference k for its continuation. By Theorem **??**, the path can be decomposed into a form required by case 2 or case 3. In case 2, $\bar{c}$ was born at inner call $\overline{\text{UEI}}$ and passed in an arbitrary number of tail calls before the tail or continuation call of $\overline{\text{EE}}$. Case 3 is like case 2 except that $\bar{c}$ is $halt$.

The function $btime$ is correct if the timestamp on the terminal state of the path it produces is the same as the birth time of the continuation of the terminal state of the path it's given. We define some supporting notation before we express it formally.

Definition 2. *Let* $q_{call} = q$ *for* $call = (f\, e^*\, q)$ *or* $call = (q\, e^*)$.

Definition 3 (Continuation Birth Timestamp)**.**

$$\overline{btime}((lam, \beta, t)) = t$$
$$\overline{btime}(halt) = t_0$$

Definition 4 (Continuation Procedure)**.**

$$CP(\overline{\text{UA}}) = \bar{c} \text{ where } \overline{\text{UA}} = (\overline{proc}, \langle \bar{d}_1, \ldots, \bar{d}_n, \bar{c}\rangle, \overline{ve}, \delta, t)$$
$$CP(\overline{\text{CA}}) = \bar{c} \text{ where } \overline{\text{CA}} = (\bar{c}, \overline{\mathbf{d}}, \overline{ve}, \delta, t)$$

Definition 5 (Invocation Continuation)**.**

$$IC(\overline{\text{E}}) = \overline{ve}(k, \beta(k)) \text{ where } \overline{\text{E}} = (call, \beta, \overline{ve}, \delta, t)$$
$$IC(\overline{\text{CA}}) = \overline{ve}(k, \beta(k)) \text{ where } \overline{\text{CA}} = ((clam, \beta, t_c), \overline{\mathbf{d}}, \overline{ve}, \delta, t)$$

where $k \in \text{dom}(\beta)$

Lemma 1. *If* $\overline{\text{UA}} \Rightarrow^+ \bar{\varsigma}$ *where* $\overline{\text{UA}} \in CE(\bar{\varsigma})$*, then* $IC(\bar{\varsigma}) = CP(\overline{\text{UA}})$.

Proof. By induction on $CE(\cdot)$.

1. Case $\overline{\text{UA}} \Rightarrow^0 \overline{\text{UA}}$:
   Doesn't apply.
2. Case $\overline{\text{UA}} \Rightarrow^* \bar{\varsigma}' \Rightarrow \bar{\varsigma}$ where $\bar{\varsigma}' \notin \overline{UEval} \cup \overline{CEvalExit}$:
   There are three cases:
   (a) Case $\bar{\varsigma}' = \overline{\text{UA}}$:
   By $\overline{\text{UA}} \Rightarrow \bar{\varsigma}$, the continuation is bound.
   (b) Case $\bar{\varsigma}' = \overline{\text{UA}}$:
   By $\overline{\text{CA}} \Rightarrow \bar{\varsigma}$, the environment is restored.
   (c) Case $\bar{\varsigma}' = \overline{\text{CEI}}$:
   By $\overline{\text{CEI}} \Rightarrow \bar{\varsigma}$, the environment is captured.
3. Case $\overline{\text{UA}} \Rightarrow^+ \bar{\varsigma}' \Rightarrow \overline{\text{UA}_0} \Rightarrow \overline{\text{CEE}} \Rightarrow \bar{\varsigma}$ where $\overline{\text{UA}} = CE(\bar{\varsigma}')$, $\bar{\varsigma}' = \overline{\text{UEI}}$ where $\overline{\text{UEI}} = ((f\, e^*\, clam), \beta, \overline{ve}, \delta, t)$, and $\overline{\text{UA}_0} \in CE^*(\overline{\text{CEE}})$. By $\overline{\text{UEI}} \Rightarrow \overline{\text{UA}_0}$, $CP(\overline{\text{UA}}) = \overline{\mathcal{A}}(clam, \beta, \overline{ve}, t)$. By Lemma 2 and $\overline{\text{CEE}} \Rightarrow \bar{\varsigma}$, $CP(\bar{\varsigma}) = \overline{\mathcal{A}}(clam, \beta, \overline{ve}, t)$. Then $IC(\bar{\varsigma}) = CP(\overline{\text{UA}})$.

□

Lemma 2. *If* $\overline{\text{UA}} \Rightarrow^+ \overline{\text{CEE}}$ *where* $\overline{\text{UA}} \in CE^*(\overline{\text{CEE}})$ *and* $\overline{\text{CEE}} = ((k\, e^*)_\gamma, \beta, \overline{ve}, \delta, t)$*, then* $\overline{\mathcal{A}}(k, \beta, \overline{ve}, t) = CP(\overline{\text{UA}})$.

Proof. By induction on $CE^*(\cdot)$.

1. Case $\overline{\text{UA}} = CE(\overline{\text{CEE}})$:
   By Lemma 1, $IC(\overline{\text{CEE}}) = CP(\overline{\text{UA}})$. By definition, $\overline{\mathcal{A}}(k, \beta, \overline{ve}, t) = \overline{ve}(k, \beta(k))$. By definition, $IC(\overline{\text{CEE}}) = \overline{ve}(k, \beta(k))$. Then $\overline{\mathcal{A}}(k, \beta, \overline{ve}, t) = CP(\overline{\text{UA}})$.
2. Case $\overline{\text{UA}} \Rightarrow^+ \overline{\text{UEE}} \Rightarrow \overline{\text{UA}_0} \Rightarrow^+ \overline{\text{CEE}}$ where $\overline{\text{UA}} = CE(\overline{\text{UEE}})$ and $\overline{\text{UA}_0} \in CE^*(\overline{\text{CEE}})$:
   By Lemma 1 and above reasoning, $IC(\overline{\text{UEE}}) = CP(\overline{\text{UA}})$. By $\overline{\text{UEE}} \Rightarrow \overline{\text{UA}_0}$, $CP(\overline{\text{UA}_0}) = IC(\overline{\text{UEE}})$. By induction, $\overline{\mathcal{A}}(k, \beta, \overline{ve}, t) = CP(\overline{\text{UA}_0})$. Then $\overline{\mathcal{A}}(k, \beta, \overline{ve}, t) = CP(\overline{\text{UA}})$.

□

Theorem 1 (Continuation Birth Time Correctness)**.** *If* $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{E}}$ *where* $\overline{\text{E}} = (call, \beta, \overline{ve}, \delta, t)$ *and* $\bar{P}' = btime(\bar{P})$*, then* $\overline{btime}(\overline{\mathcal{A}}(q_{call}, \beta, \overline{ve}, t)) = t_{\bar{P}'}$.

Proof. Let $\overline{\text{E}} = (call, \beta, \overline{ve}, \delta, t)$.
Consider cases of $btime$.

1. Case $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{EI}}$:
   By assumption, $q_{call} = clam$ so $\overline{\mathcal{A}}(q_{call}, \beta, \overline{ve}, t) = \overline{\mathcal{A}}(clam, \beta, \overline{ve}, t)$. By definition, $\overline{\mathcal{A}}(clam, \beta, \overline{ve}, t) = (clam, \beta, t)$. By definition, $\overline{btime}((clam, \beta, t)) = t$. By definition, $btime(\bar{P}) = \bar{P}$. By definition, $btime(\bar{P}) = \bar{P}$ and $t_{\bar{P}} = t$.
2. Case $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{UEI}} \Rightarrow \overline{\text{UA}} \Rightarrow^+ \overline{\text{EE}}$ where $\overline{\text{UA}} \in CE^*(\overline{\text{EE}})$:
   By assumption, $q_{call} = k$ so, by Lemma 2, $\overline{\mathcal{A}}(k, \beta, \overline{ve}, t) = CP(\overline{\text{UA}})$. By definition, $btime(\bar{P}) = \bar{P}' \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{UEI}}$. By $\overline{\text{UEI}} \Rightarrow \overline{\text{UA}}$, the result follows with reasoning from the case above.
3. Case $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^0 \overline{\text{UA}} \Rightarrow^+ \overline{\text{EE}}$ where $\overline{\text{UA}} \in CE^*(\overline{\text{EE}})$:
   By assumption, $q_{call} = k$ so, by Lemma 2, $\overline{\mathcal{A}}(k, \beta, \overline{ve}, t) = CP(\overline{\text{UA}})$. By definition, $btime(\bar{P}) = \bar{P}' \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^0 \overline{\text{UA}}$. By definition of $\overline{\mathcal{I}}$, $CP(\overline{\text{UA}}) = halt$. By definition, $\overline{btime}(halt) = t_0$. By definition of $\overline{\mathcal{I}}$, $t_{\overline{\text{UA}}} = t_0$. Then $t_{\bar{P}'} = t_0$.

□

3.2 Log Recovery

We now show that the ability to recover continuation birth times allows us to recover the log itself. We recover logs inductively on an evaluation path: to recover the log δ' of $\bar{\varsigma}'$, we first recover the log δ of the predecessor $\bar{\varsigma}$ of $\bar{\varsigma}'$; the log of $\overline{\mathcal{I}}(pr, \overline{\mathbf{d}})$ is known by definition.

Definition 6 (Log Recovery)**.**

$$Rec(\bar{P}) = \bot_\delta[t_0 \mapsto \epsilon]$$

if $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^0 \bar{\varsigma}$.

$$Rec(\bar{P}') = (\lambda t.\delta(t) + p_\Delta)[t_{\bar{\varsigma}'} \mapsto \epsilon]$$

if $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^* \bar{\varsigma}$ *and* $\bar{P}' \equiv \bar{P} \Rightarrow \bar{\varsigma}'$ *where* $\delta = Rec(\bar{P})$ *and*

$$p_\Delta = \begin{cases} \left\langle {}^{\psi}_{t} \right| & \text{if } \bar{\varsigma} = \overline{\text{A}} \text{ where } \overline{\text{A}} = (L(\psi), \_, \_, \_, t) \\ \lfloor \delta(t_{\overline{\text{E}}'}) \rfloor^{-1} & \text{if } \bar{\varsigma} = \overline{\text{E}} \text{ and } btime(\bar{P}) = \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow \overline{\text{E}'} \end{cases}$$

Log recovery is correct if the log we construct is the same as the log of the state. We express this condition in the following theorem.

Theorem 2 (Genuine Log Recovery)**.** *For all* $n \in \mathbb{N}$*, if* $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^n \bar{\varsigma}$ *, then* $Rec(\bar{P})$=$\delta_{\bar{\varsigma}}$.

The proof proceeds inductively over path length and by cases on the terminal state at each inductive step. Unsurprisingly, Theorem **??** is fundamental to the $\overline{\text{E}}$ case.

Proof. By induction on n.

1. Base case $P \equiv \mathcal{I}(pr, \mathbf{d}) \to^0 \varsigma$:
   $\delta_P = \bot_\delta[t \mapsto \epsilon] = \emptyset_\delta[t_{\bar{\varsigma}} \mapsto \epsilon] = \delta_{\bar{\varsigma}}$
2. Inductive case $P \equiv \mathcal{I}(pr, \mathbf{d}) \to \varsigma$ and $P' \equiv P \to \varsigma'$:
   Let $\delta = Rec(P)$. By induction, $\delta = \delta_{\bar{\varsigma}}$.
   By cases on ς:
   (a) Case $\varsigma = \text{A}$:
   By definition, $Rec(P') = (\lambda t.\delta(t) + p_\Delta)[\varsigma' \mapsto \epsilon]$ where $p_\Delta = \left\langle {}^{\psi}_{\varsigma'} \right|$ where $\psi = LAB(\varsigma)$.

(b) Case $\varsigma = \text{E}$:
By definition, $Rec(P') = (\lambda t.\delta(t) + p_\Delta)[\varsigma' \mapsto \epsilon]$ where $p_\Delta = \lfloor \delta(P_*) \rfloor^{-1}$ where $P_* = btime(P)$. By Theorem **??**, $\lfloor \delta(P_*) \rfloor^{-1} = \lfloor \delta_t(t_{\bar{P}_*}) \rfloor^{-1}$.
Then $Rec(P') = \delta_{\bar{P}'}$.

□

3.3 Invocation Frame Strings

Because frame strings capture the actions a stack performs to manage the environment, it should not be surprising that, when a procedure exits, the net stack action taken is to pop its—and only its–environment frames off the stack. This fact is captured by the following lemmas.

Lemma 3. *If* $\text{A} \Rightarrow \text{E}$, *then* $\text{A} \rightarrow \text{E}$.

Lemma 4. *If* $\text{UA} \Rightarrow \text{E} \Rightarrow \text{CA}_1 \Rightarrow \text{E}_1 \Rightarrow \cdots \Rightarrow \text{CA}_n \Rightarrow \text{E}_n$, *then* $\lfloor [t_{\text{UA}}, t_{\text{E}_n}] \rfloor = \langle^{\ell}_{t_\text{E}} | \langle^{\gamma_1}_{t_{\text{E}_1}} | \ldots \langle^{\gamma_n}_{t_{\text{E}_n}} |$ *where* $\text{UA} = (L(\ell), \_, \_, \_)$ *and* $\text{CA}_i = (L(\gamma_i), \_, \_, \_)$ *for* $1 \le i \le n$.

Proof. By induction on n.

- Case $n = 0$:
  Then $\text{E} = \text{EE}$. By Lemma 3, $\text{UA} \rightarrow \text{EE}$. By definition, $\lfloor [t_{\text{UA}}, t_{\text{EE}}] \rfloor = \langle^{\ell}_{\text{EE}} |$.
- Case $n = k$:
  By assumption, we have $\text{UA} \longrightarrow \text{E} \longrightarrow \text{CA}_1 \longrightarrow \text{E}_1 \longrightarrow \cdots \longrightarrow \text{CA}_k \longrightarrow \text{E}_k \longrightarrow \text{CA}_{k+1} \longrightarrow \text{E}_{k+1}$ and $\lfloor [t_{\text{UA}}, t_{\text{E}_k}] \rfloor = \langle^{\ell}_{\text{E}} | \langle^{\gamma_1}_{\text{E}_1} | \ldots \langle^{\gamma_k}_{\text{E}_k} |$.
  By cases on E_k.
  - Case $\text{E}_k = \text{EE}$:
    This case can't happen by assumption.
  - Case $\text{E}_k = \text{CEI}$:
    The continuation is born in this state, so no frames are popped. At CA_{k+1}, the just born continuation is invoked, and its frame is pushed.
  - Case $\text{E}_k = \text{UEI}$:
    The continuation is born in this state, so no frames are popped. By assumption, we have $\text{UEI} \rightarrow \text{UA}_0 \rightarrow^+ \text{CEE} \rightarrow \text{CA}_{k+1}$ where $\text{UA}_0 \in CE^*(\text{CEE})$. By induction, we have that, by $\text{CEE} \rightarrow \text{CA}_{k+1}$, the frame string change is the inverse of the pushed frames.

□

Lemma 5. *If* $\text{UA} \rightarrow^+ \text{CEE} \rightarrow \text{CA}$ *where* $\text{UA} \in CE^*(\text{CEE})$, *then* $\lfloor \delta_{\text{CA}}(\text{UA}) \rfloor = \epsilon$.

Proof. By induction on $CE^*(\cdot)$.

- Case $\text{UA} = CE(\text{CEE})$:
  By the above.
- Case $\text{UA} \rightarrow^+ \text{UEE} \rightarrow \text{UA}_0 \rightarrow^+ \text{CEE}$ where $\text{UA} = CE(\text{UEE})$ and $\text{UA}_0 \in CE^*(\text{CEE})$:
  By the above, we have the log change for $\text{UA} \rightarrow^+ \text{UEE}$. By $\text{UEE} \rightarrow \text{UA}_0$, the net log change here is empty. By induction, the net log change is empty.

□

4. Binding- and Birth-State Resolution Correctness

Lemma 6 ($BirthBP$ Correctness)**.** *If*

1. $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^* \overline{\text{UA}}$ *where* $\overline{\text{UA}} = (\overline{proc}, \langle \bar{d}_1, \ldots, \bar{d}_n, \bar{c} \rangle, \overline{ve}, \delta, t)$, *or*
2. $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^* \overline{\text{CA}}$ *where* $\overline{\text{CA}} = (\overline{proc}, \langle \bar{d}_1, \ldots, \bar{d}_n \rangle, \overline{ve}, \delta, t)$,

then $BirthBP(\bar{P}, u) = \bar{P}_* \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{E}_*}$ *such that* $\overline{btime}(\bar{d}_i) = t_{\overline{\text{E}_*}}$ *where* $i = BP_{\overline{proc}}(u,)$*.*

Proof. By induction on $BirthIP(\bar{P}, i)$. □

Lemma 7 ($BirthIP$ Correctness)**.** *If*

1. $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^* \overline{\text{UA}}$ *where* $\overline{\text{UA}} = (\overline{proc}, \langle \bar{d}_1, \ldots, \bar{d}_n, \bar{c} \rangle, \overline{ve}, \delta, t)$, *or*
2. $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^* \overline{\text{CA}}$ *where* $\overline{\text{CA}} = (\overline{proc}, \langle \bar{d}_1, \ldots, \bar{d}_n \rangle, \overline{ve}, \delta, t)$,

then $BirthIP(\bar{P}, i) = \bar{P}_* \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{E}_*}$ *such that* $\overline{btime}(\bar{d}_i) = t_{\overline{\text{E}_*}}$.

Proof. If $n = 0$, then it is vacuously true. If $n > 0$, then $\bar{P} \equiv \bar{P}' \Rightarrow \overline{\text{A}}$ where $\bar{P}' \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow \overline{\text{E}}$. If $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{UE}} \Rightarrow \overline{\text{UA}}$, then, by $\overline{\text{UE}} \Rightarrow \overline{\text{UA}}$, $\bar{d}_i = \overline{\mathcal{A}}(e_i, \beta, \overline{ve}, t)$ where $\overline{\text{UE}} = ((f\, e_1\, \ldots\, e_n\, q), \beta, \overline{ve}, \delta, t)$. If $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{CE}} \Rightarrow \overline{\text{CA}}$, then, by $\overline{\text{CE}} \Rightarrow \overline{\text{CA}}$, $\bar{d}_i = \overline{\mathcal{A}}(e_i, \beta, \overline{ve}, t)$ where $\overline{\text{CE}} = ((q\, e_1\, \ldots\, e_n), \beta, \overline{ve}, \delta, t)$. Then the result follows by induction on $BirthIE(\bar{P}', i)$. □

Lemma 8 ($BirthIE$ Correctness)**.** *If*

1. $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{UE}}$ *where* $\overline{\text{UE}} = ((f\, e_1\, \ldots\, e_n\, q), \beta, \overline{ve}, \delta, t)$, *or*
2. $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{CE}}$ *where* $\overline{\text{CE}} = ((q\, e_1\, \ldots\, e_n), \beta, \overline{ve}, \delta, t)$

then $BirthIP(\bar{P}, i) = \bar{P}_* \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{E}_*}$ *such that* $\overline{btime}(\overline{\mathcal{A}}(e_i, \beta, \overline{ve}, t)) = t_{\overline{\text{E}_*}}$ *for* $1 \le i \le n$*.*

Proof. If $n = 0$, then it is vacuously true. If $n > 0$, then, by definition, $BirthIE(\bar{P}, i) = Birth(\bar{P}, e_i)$. The result follows by induction on $Birth(\bar{P}, e_i)$. □

Lemma 9 ($BirthOP$ Correctness)**.** *If* $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^* \overline{\text{UA}}$ *where* $\overline{\text{UA}} = (\overline{proc}, \langle \bar{d}_1, \ldots, \bar{d}_n, \bar{c} \rangle, \overline{ve}, \delta, t)$, *then* $BirthOP(\bar{P}) = \bar{P}_* \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{E}_*}$ *such that* $\overline{btime}(\overline{proc}) = t_{\overline{\text{E}_*}}$*.*

Proof. If $n = 0$, then it is vacuously true. If $n > 0$, then $\bar{P} \equiv \bar{P}' \Rightarrow \overline{\text{UA}}$ where $\bar{P}' \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow \overline{\text{UE}}$. By $\bar{P} \equiv \overline{\text{UE}} \Rightarrow \overline{\text{UA}}$, $\overline{proc} = \overline{\mathcal{A}}(f, \beta', \overline{ve}', t')$ where $\overline{\text{UE}} = ((f\, e^*\, q), \beta', \overline{ve}', \delta', t')$. Then the result follows by induction on $BirthOE(\bar{P}')$. □

Lemma 10 ($BirthOE$ Correctness)**.** *If* $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{UE}}$ *where* $\overline{\text{UE}} = ((f\, e_1\, \ldots\, e_n\, q), \beta, \overline{ve}, \delta, t)$*, then then* $BirthIP(\bar{P}, i) = \bar{P}_* \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{E}_*}$ *such that* $\overline{btime}(\overline{\mathcal{A}}(f, \beta, \overline{ve}, t)) = t_{\overline{\text{E}_*}}$*.*

Proof. By definition, $BirthOE(\bar{P}) = Birth(\bar{P}, f)$. The result follows by induction on $Birth(\bar{P}, f)$. □

Lemma 11 ($Birth$ Correctness)**.** *If* $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{E}}$ *where* $\overline{\text{E}} = (call, \beta, \overline{ve}, \delta, t)$*, and* $Birth(\bar{P}, h) = \bar{P}_* \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{E}_*}$*, then* $\overline{btime}(\overline{\mathcal{A}}(h, \beta, \overline{ve}, t)) = t_{\overline{\text{E}_*}}$*.*

Proof. By cases on h.

- Case $h = ulam$: By definition, $Birth(\bar{P}, ulam) = \bar{P}$. Then $t_{\overline{\text{E}_*}} = t_{\overline{\text{E}}} = t$. By definition $\overline{\mathcal{A}}(ulam, \beta, \overline{ve}, t) = (ulam, \beta, t)$. By definition, $\overline{btime}((ulam, \beta, t)) = t$. Then $\overline{btime}(\overline{\mathcal{A}}(ulam, \beta, \overline{ve}, t)) = t_{\overline{\text{E}_*}}$.
- Case $h = u$: By definition, $Birth(\bar{P}, u) = BirthBP(\bar{P}_2, u)$ where $\bar{P}_1 = Bind(\bar{P}, u)$ such that $\bar{P}_1 \equiv \bar{P}_2 \Rightarrow \overline{\text{E}_1}$ and $\bar{P}_2 \equiv \bar{P}_1 \Rightarrow \overline{\text{A}_1}$. By induction on $Bind(\bar{P}, u)$, $\beta(u) = t_{\overline{\text{E}_1}}$. Then $\overline{ve}(u, \beta(u)) = \overline{ve}_{\overline{\text{E}_1}}(u, t_{\overline{\text{E}_1}})$. By $\overline{\text{A}_1} \Rightarrow \overline{\text{E}_1}$, $\overline{ve}_{\overline{\text{E}_1}}(u, t_{\overline{\text{E}_1}}) = \pi_i(\overline{\mathbf{d}})$ where $\overline{\text{A}_1} = (\overline{proc}, \overline{\mathbf{d}}, \overline{ve}_1, \delta_1, t_1)$ and $i = BP_{\overline{proc}}(u,)$. By induction, $BirthBP(\bar{P}_2, u) = \bar{P}_* \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow \overline{\text{E}_*}$ such that $\overline{btime}(\pi_i(\overline{\mathbf{d}})) = t_{\overline{\text{E}_*}}$. As $\pi_i(\overline{\mathbf{d}}) = \overline{ve}_{\overline{\text{E}_1}}(u, t_{\overline{\text{E}_1}}) = \overline{ve}(u, \beta(u)) = \overline{\mathcal{A}}(u, \beta, \overline{ve}, t)$, $\overline{btime}(\overline{\mathcal{A}}(u, \beta, \overline{ve}, t)) = t_{\overline{\text{E}_*}}$ and we have our result.

□

Lemma 12 ($Bind$ Correctness)**.** *If $\bar{P}' \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{E}}$ where $\overline{\text{E}} = (call, \beta, \overline{ve}, \delta, t)$ and $Bind(\bar{P}', u) = \bar{P}_* \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{E}_*}$, then $\beta(u) = t_{\overline{\text{E}_*}}$.*

Proof. Let $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^* \overline{\text{A}}$ such that $\bar{P}' \equiv logpath \Rightarrow \overline{\text{E}}$. By cases on $Bind(\bar{P}, u)$.

- Case $u \in B(\bar{P}_1)$: By definition, $Bind(\bar{P}', u) = \bar{P}'$ with $\overline{\text{E}_*} = \overline{\text{E}}$. By $\overline{\text{A}} \Rightarrow \overline{\text{E}}$, $\beta(u) = t_{\overline{\text{E}_*}}$.
- Case $u \notin B(\bar{P})$: By definition, $Bind(\bar{P}', u) = Find(\bar{P}', u)$. By induction, $Find(\bar{P}', u) = \bar{P}_* \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{E}_*}$ where $\beta(u) = t_{\overline{\text{E}_*}}$.

□

Lemma 13 ($Find$ Correctness)**.** *If $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^* \overline{\text{A}}$ such that $u \notin B(\bar{P})$, $\bar{P}' \equiv \bar{P} \Rightarrow \overline{\text{E}}$ where $\overline{\text{E}} = (call, \beta, \overline{ve}, \delta, t)$, and $Find(\bar{P}', u) = \bar{P}_* \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{E}_*}$, then $\beta(u) = t_{\overline{\text{E}_*}}$.*

Proof. By cases on $Find(\bar{P}, u)$.

1. Case $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^* \overline{\text{UA}}$: Let $\overline{\text{UA}} = (\overline{proc}, \overline{\mathbf{d}}, \overline{ve}', \delta', t')$. By assumption, $u \notin B(\bar{P})$, so $\beta(u) = \beta_{\overline{proc}}(u)$. By definition, $Find(\bar{P}', u) = Bind(BirthOP(\bar{P}), u)$. By induction, $BirthOP(\bar{P}) = \bar{P}_1 \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{E}_1}$ such that $\overline{btime}(\overline{proc}) = t_{\overline{\text{E}_1}}$. By definition of $\Rightarrow$, $\beta_{\overline{proc}}(u) = \beta_{\overline{\text{E}_1}}(u)$. The result follows by induction on $Bind(\bar{P}_1, u)$.
2. Case $\bar{P} \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow^+ \overline{\text{E}_1} \Rightarrow^+ \overline{\text{CA}}$: Let $\overline{\text{CA}} = (\bar{c}, \overline{\mathbf{d}}, \overline{ve}', \delta', t')$. By assumption, $\overline{\text{E}_1} \Longrightarrow \overline{\text{CA}}$ and $u \notin B(\bar{P})$, so $\beta(u) = \beta_{\overline{\text{E}_1}}(u)$. The result follows by induction on $Bind(\bar{P}_1, u)$ where $\bar{P}_1 \equiv \overline{\mathcal{I}}(pr, \overline{\mathbf{d}}) \Rightarrow \overline{\text{E}_1}$.

□