Multi-Continuation Pushdown Analysis Technical Report

Kimball Germane and Matthew Might

University of Utah

1 Abstraction Soundness

Theorem 1 (Simulation).
If $\varsigma \to \varsigma'$ *and* $|\varsigma|_{ca} \sqsubseteq \hat{\varsigma}$*, then there exists* $\hat{\varsigma}'$ *such that* $\hat{\varsigma} \leadsto \hat{\varsigma}'$ *and* $|\varsigma'|_{ca} \sqsubseteq \hat{\varsigma}'$*.*

Proof. By cases on ς.

1. Case $\varsigma = \text{UE}$:
   $\text{UE} = ((f\,\boldsymbol{e}\,\boldsymbol{q}^+)_\gamma, \beta_u, \beta_k, st, ve, t)$ and
   $\hat{\text{UE}} = ((f\,\boldsymbol{e}\,\boldsymbol{q}^+)_\gamma, \widehat{st}, h)$ where
   $|ve|_{ca} \sqsubseteq h$ so $|proc = \mathcal{A}_u(f, \beta_u, ve)|_{ca} \sqsubseteq \hat{\mathcal{A}}(f, h) \ni ulam$ and $|\boldsymbol{d} = \mathcal{A}_u(\boldsymbol{e}, \beta_u, ve)|_{ca} \sqsubseteq \hat{\mathcal{A}}(\boldsymbol{e}, h) = \hat{\boldsymbol{d}}$;
   $\boldsymbol{c} = \mathcal{A}_k(\boldsymbol{q}, \beta_k, st)$, $reconstruct(CP(\gamma), \beta_k, st) = \widehat{st}$, and Lemma 1 so $pop(\boldsymbol{c}, (\beta_u, \beta_k) :: st) = st'$, $(\hat{\boldsymbol{q}}, \widehat{st}') = reconstruct^*(\boldsymbol{c}, st')$, and $(\hat{\boldsymbol{q}}, \widehat{st}') = \widehat{pop}(\boldsymbol{q}, \widehat{st})$;
   so $|(proc, \boldsymbol{d}, \boldsymbol{c}, st', ve, t')|_{ca} \sqsubseteq (ulam, \hat{\boldsymbol{d}}, \hat{\boldsymbol{q}}, \widehat{st}', h)$
2. Case $\varsigma = \text{CE}$:
   $\text{CE} = ((q\,\boldsymbol{e})_\gamma, \beta_u, \beta_k, st, ve, t)$ and
   $\hat{\text{CE}} = ((q\,\boldsymbol{e})_\gamma, \widehat{st}, h)$ where
   $|ve|_{ca} \sqsubseteq h$ so $|\boldsymbol{d} = \mathcal{A}_u(\boldsymbol{e}, \beta_u, ve)|_{ca} \sqsubseteq \hat{\mathcal{A}}(\boldsymbol{e}, h) = \hat{\boldsymbol{d}}$;
   $(cp, fp) = c = \mathcal{A}_k(q, \beta_k, st)$, $reconstruct(CP(\gamma), \beta_k, st) = \widehat{st}$, and Lemma 1 so $pop(\langle c \rangle, (\beta_u, \beta_k) :: st) = st'$, $(\langle cp \rangle, \widehat{st}') = reconstruct^*(\langle (cp, |st|) \rangle, st')$, and $(\langle cp \rangle, \widehat{st}') = \widehat{pop}(\langle q \rangle, \widehat{st})$;
   so $|(cp, \boldsymbol{d}, st', ve, t')|_{ca} \sqsubseteq (cp, \hat{\boldsymbol{d}}, \widehat{st}, h)$
3. Case $\varsigma = \text{UA}$:
   $\text{UA} = (proc, \boldsymbol{d}, \boldsymbol{c}, st, ve, t)$ and
   $\hat{\text{UA}} = (ulam, \hat{\boldsymbol{d}}, \hat{\boldsymbol{q}}, \widehat{st}, h)$ where
   $|proc|_{ca} = \{ulam = (\lambda\,(\boldsymbol{u}\,\boldsymbol{k}^+)\,call)_\gamma\}$,
   $(\hat{\boldsymbol{q}}, \widehat{st}) = reconstruct^*(\boldsymbol{c}, st)$ so $reconstruct(CP(call), \beta_k, st) = reconstruct(\boldsymbol{k}, [\boldsymbol{k} \mapsto \boldsymbol{c}], st) = [\boldsymbol{k} \mapsto \hat{\boldsymbol{q}}] :: \widehat{st} = \widehat{st}'$, and
   $|ve|_{ca} \sqsubseteq h$ and $|\boldsymbol{d}|_{ca} \sqsubseteq \hat{\boldsymbol{d}}$ so $|ve'|_{ca} = |ve[(\boldsymbol{u}, t') \mapsto \boldsymbol{d}]|_{ca} = |ve|_{ca} \sqcup |[(\boldsymbol{u}, t') \mapsto \boldsymbol{d}]|_{ca} \sqsubseteq h \sqcup [\boldsymbol{u} \mapsto \hat{\boldsymbol{d}}] = h'$
   so $|(call, \beta'_u, \beta_k, st, ve', t')|_{ca} \sqsubseteq (call, \widehat{st}', h')$
4. Case $\varsigma = \text{CA}$:
   $\text{CA} = (clam, \boldsymbol{d}, st, ve, t)$ and
   $\hat{\text{CA}} = (clam, \hat{\boldsymbol{d}}, \widehat{st}, h)$ where

$clam = (\lambda\,(\boldsymbol{u})\; call)_\gamma$,
$(\langle cp\rangle, \widehat{st}) = reconstruct^*(\langle(cp, |st|)\rangle, st)$, and
$|ve|_{ca} \sqsubseteq h$ and $|\boldsymbol{d}|_{ca} \sqsubseteq \hat{\boldsymbol{d}}$ so $|ve'|_{ca} = |ve[(\boldsymbol{u}, t') \mapsto \boldsymbol{d}]|_{ca} = |ve|_{ca} \sqcup |[(\boldsymbol{u}, t') \mapsto \boldsymbol{d}]|_{ca} \sqsubseteq h \sqcup [\boldsymbol{u} \mapsto \hat{\boldsymbol{d}}] \sqsubseteq h'$
so $|(call, \beta'_u, \beta_k, st, ve', t')|_{ca} \sqsubseteq (call, \widehat{st}, h')$

Definition 1 *A stack st is* well-formed *if, for every continuation environment β_k at stack level n, the frame pointer fp of each continuation c in β_k is less than n.*

Lemma 1. *Suppose $|\mathrm{UE}|_{ca} \sqsubseteq \hat{\mathrm{UE}}$ where $\mathrm{UE} = ((f\,\boldsymbol{e}\,\boldsymbol{q}^+)_\gamma, \beta_u, \beta_k, st, ve, t)$ and UE is well-formed. If $\boldsymbol{k} = CP(\gamma)$, $\mathcal{A}_k(\boldsymbol{q}, \beta_u, st) = \boldsymbol{c}$, $reconstruct(\boldsymbol{k}, \beta_k, st) = \widehat{st}$, and $pop(\boldsymbol{c}, (\beta_u, \beta_k) :: st) = st'$, then $reconstruct^*(\boldsymbol{c}, st') = \widehat{pop}(\boldsymbol{q}, \widehat{st})$.*

Proof. By induction on st.

1. Base case $st = \langle\rangle$:
$reconstruct(\boldsymbol{k}, \beta_k, \langle\rangle) = [\boldsymbol{k} \mapsto \mathbf{halt}] :: \langle\rangle \Leftarrow reconstruct^*((\mathbf{halt}, 0), \langle\rangle) = (\mathbf{halt}, \langle\rangle)$
If $\boldsymbol{q} = \boldsymbol{k}'$, then $pop(\boldsymbol{c}, (\beta_u, \beta_k) :: \langle\rangle) = pop((\mathbf{halt}, 0), (\beta_u, \beta_k) :: \langle\rangle) = \langle\rangle$ and $reconstruct^*((\mathbf{halt}, 0), \langle\rangle) = (\mathbf{halt}, \langle\rangle) = \widehat{pop}(\boldsymbol{k}', [\boldsymbol{k} \mapsto \mathbf{halt}] :: \langle\rangle)$.
Otherwise, $pop(\boldsymbol{c}, (\beta_u, \beta_k) :: \langle\rangle) = (\beta_u, \beta_k) :: \langle\rangle$ and $reconstruct^*(\boldsymbol{c}, (\beta_u, \beta_k) :: \langle\rangle) = (\boldsymbol{q}, [\boldsymbol{k} \mapsto \mathbf{halt}] :: \langle\rangle) = \widehat{pop}(\boldsymbol{q}, [\boldsymbol{k} \mapsto \mathbf{halt}] :: \langle\rangle)$.
2. Inductive case $st = (\beta'_u, \beta'_k) :: st_k$:
$reconstruct(\boldsymbol{k}, \beta_k, (\beta'_u, \beta'_k) :: st_k) = [\boldsymbol{k} \mapsto \hat{\boldsymbol{q}}] :: \widehat{st}_k \Leftarrow reconstruct^*(\boldsymbol{c}, st_k) = (\hat{\boldsymbol{q}}, \widehat{st}_k)$
If $\boldsymbol{q} = \boldsymbol{k}'$, then $pop(\boldsymbol{c}, (\beta_u, \beta_k) :: (\beta'_u, \beta'_k) :: st_k) = pop(\boldsymbol{c}, (\beta'_u, \beta'_k) :: st_k) = st'_k$ and $reconstruct^*(\boldsymbol{c}, st'_k) = (\hat{\boldsymbol{q}}, \widehat{st}'_k) = \widehat{pop}(\boldsymbol{k}', [\boldsymbol{k} \mapsto \hat{\boldsymbol{q}}] :: \widehat{st}_k)$.
Otherwise, $pop(\boldsymbol{c}, (\beta_u, \beta_k) :: (\beta'_u, \beta'_k) :: st_k) = (\beta_u, \beta_k) :: (\beta'_u, \beta'_k) :: st_k$ and $reconstruct^*(\boldsymbol{c}, (\beta_u, \beta_k) :: (\beta'_u, \beta'_k) :: st_k) = (\boldsymbol{q}, [\boldsymbol{k} \mapsto \mathbf{halt}] :: \widehat{st}_k) = \widehat{pop}(\boldsymbol{q}, [\boldsymbol{k} \mapsto \hat{\boldsymbol{q}}] :: \widehat{st}_k)$.

The following lemma establishes that calls are more conservative than exits: a user call with a continuation argument q will pop at most as many frames as a continuation call with operator q; moreover, the positional continuation mapping is preserved on the stack.

Lemma 2 (Conservative Pop).
Let $\hat{q} = \pi_i(\hat{\boldsymbol{q}})$. If $\widehat{pop}(\langle\hat{q}\rangle, \widehat{st}) = (\langle clam\rangle, \widehat{st}_0)$ and $\widehat{pop}(\hat{\boldsymbol{q}}, \widehat{st}) = (\hat{\boldsymbol{q}}', \widehat{st}')$, then $\widehat{pop}(\langle\pi_i(\hat{\boldsymbol{q}}')\rangle, \widehat{st}') = (\langle clam\rangle, \widehat{st}_0)$.

Proof. By cases on $\hat{q}$.

- Case $\hat{q} = clam$: By definition, $\widehat{pop}(\hat{\boldsymbol{q}}, \widehat{st}) = (\hat{\boldsymbol{q}}, \widehat{st})$. Then $\widehat{pop}(\langle\pi_i(\hat{\boldsymbol{q}}')\rangle, \widehat{st}') = \widehat{pop}(\langle\pi_i(\hat{\boldsymbol{q}})\rangle, \widehat{st}) = \widehat{pop}(\langle q\rangle, \widehat{st}) = (\langle clam\rangle, \widehat{st}_0)$, by assumption.
- Case $q = k$: By induction on whether $\pi_i(\hat{\boldsymbol{q}}) = clam$ for some i. If so, then $\widehat{pop}(\hat{\boldsymbol{q}}, \widehat{st}) = (\hat{\boldsymbol{q}}, \widehat{st})$. If not, then $\widehat{pop}(\hat{\boldsymbol{q}}, \widehat{st}) = \widehat{pop}(\hat{\boldsymbol{q}}, sm :: \widehat{st}'') = \widehat{pop}(sm(\hat{\boldsymbol{q}}), \widehat{st}'')$ and the result follows by induction.

Lemma 3 (Conservative Path).

Suppose $\hat{\text{UA}} \equiv_p \hat{\text{CEE}}$ *by* n *where* $\hat{\text{UA}} = (ulam, \hat{\boldsymbol{d}}, \hat{\boldsymbol{q}}, \widehat{st}, h)$ *and* $CV(\hat{\text{CEE}}) = k$. *If* $\widehat{pop}(\langle \pi_n(\hat{\boldsymbol{q}})\rangle, \widehat{st}) = (\langle clam\rangle, \widehat{st}')$, *then* $\widehat{pop}(\langle k\rangle, \widehat{st}_{\hat{\text{CEE}}}) = (\langle clam\rangle, \widehat{st}')$.

Proof. By induction on the definition of $\cdot \equiv_p \cdot$ by $\cdot$.

1. Case $p \equiv \hat{\text{UA}} \rightsquigarrow \hat{\varsigma}' \rightsquigarrow^* \hat{\text{CEE}}$: By $\hat{\text{UA}} \rightsquigarrow \hat{\varsigma}'$, $\widehat{st}_{\hat{\varsigma}'} = sm :: \widehat{st}_{\hat{\text{UA}}}$ where $sm(k) = \pi_n(\hat{\boldsymbol{q}})$ where $CP(\hat{\text{UA}}, k) = n$. By Lemma 5, $\widehat{st}_{\hat{\text{CEE}}} = sm :: \widehat{st}_{\hat{\text{UA}}}$. Then $\widehat{pop}(\langle k\rangle, \widehat{st}_{\hat{\text{CEE}}}) = \widehat{pop}(\langle k\rangle, sm :: \widehat{st}_{\hat{\text{UA}}})$. By definition, $\widehat{pop}(\langle k\rangle, sm :: \widehat{st}_{\hat{\text{UA}}}) = \widehat{pop}(\langle sm(k)\rangle, \widehat{st}_{\hat{\text{UA}}})$. By the above, $\widehat{pop}(\langle sm(k)\rangle, \widehat{st}_{\hat{\text{UA}}}) = \widehat{pop}(\langle \pi_n(\hat{\boldsymbol{q}})\rangle, \widehat{st}_{\hat{\text{UA}}})$. By assumption, $\widehat{pop}(\langle \pi_n(\hat{\boldsymbol{q}})\rangle, \widehat{st}_{\hat{\text{UA}}}) = (\langle clam\rangle, \widehat{st}')$.
2. Case $p \equiv \hat{\text{UA}} \rightsquigarrow \hat{\varsigma}' \rightsquigarrow^* \hat{\text{UE}} \rightsquigarrow \hat{\text{UA}}_0 \rightsquigarrow^+ \hat{\text{CEE}}$ where the operator of $\hat{\text{UA}}$ is $(\lambda_\psi\,(\boldsymbol{u}\,k_1\,\ldots\,k_N)\,call)$, the call of $\hat{\text{UE}}$ is $(f\,\boldsymbol{e}\,q_1\,\ldots\,q_{N_0})_{\psi_0}$, and $\hat{\text{UA}}_0 \equiv_p \hat{\text{CEE}}$ by n_0:
   Let $\hat{\boldsymbol{q}}' = \langle q_1, \ldots, q_{N_0}\rangle$. By $\hat{\text{UA}} \rightsquigarrow \hat{\varsigma}'$, $\widehat{st}_{\hat{\varsigma}'} = sm :: \widehat{st}_{\hat{\text{UA}}}$ where $sm(k_n) = \pi_n(\hat{\boldsymbol{q}})$. By Lemma 5, $\widehat{st}_{\hat{\text{UE}}} = sm :: \widehat{st}_{\hat{\text{UA}}}$. By assumption, $\widehat{pop}(\langle \pi_{n_0}(\hat{\boldsymbol{q}}')\rangle, \widehat{st}_{\hat{\text{UE}}}) = \widehat{pop}(\langle k_n\rangle, sm :: \widehat{st}_{\hat{\text{UA}}})$. By above, $\widehat{pop}(\langle k_n\rangle, sm :: \widehat{st}_{\hat{\text{UA}}}) = \widehat{pop}(sm(k_n), \widehat{st}_{\hat{\text{UA}}})$. By assumption, $\widehat{pop}(\langle sm(k_n)\rangle, \widehat{st}_{\hat{\text{UA}}}) = \widehat{pop}(\langle \pi_n(\hat{\boldsymbol{q}})\rangle, \widehat{st}_{\hat{\text{UA}}})$. By definition, $\hat{\text{UE}} \rightsquigarrow (ulam_0, \hat{\boldsymbol{d}}_0, \hat{\boldsymbol{q}}_0, \widehat{st}_0, h_0)$ where $(\hat{\boldsymbol{q}}_0, \widehat{st}_0) = \widehat{pop}(\hat{\boldsymbol{q}}', \widehat{st}_{\hat{\text{UE}}})$. By Lemma 2, $\widehat{pop}(\langle \pi_{n_0}(\hat{\boldsymbol{q}}_0)\rangle, \widehat{st}_0) = (\langle clam\rangle, \widehat{st}')$. By induction, $\widehat{pop}(\langle k\rangle, \widehat{st}_{\hat{\text{CEE}}}) = (\langle clam\rangle, \widehat{st}')$.

Lemma 4 (Same Stack).

If $p \equiv \hat{\text{UE}} \rightsquigarrow \hat{\text{UA}} \rightsquigarrow^+ \hat{\text{CEE}} \rightsquigarrow \hat{\varsigma}$ *where* $call_{\hat{\text{UE}}} = (f\,\boldsymbol{e}\,q_1\,\ldots\,q_n\,\ldots\,q_N)_\ell$, $q_n \in CLam$, *and* $\hat{\text{UA}} \equiv_p \hat{\text{CEE}}$ *by* n, *then* $\widehat{st}_{\hat{\varsigma}} = sm :: \widehat{st}$ *and* $\widehat{st}_{\hat{\text{UE}}} = sm :: \widehat{st}$.

Proof. Let $\hat{\boldsymbol{q}} = \langle q_1, \ldots, q_N\rangle$ so that $\pi_n(\hat{\boldsymbol{q}}) = clam$. By $\hat{\text{UE}} \rightsquigarrow \hat{\text{UA}}$, if $S_?(f)$, Then $\widehat{pop}(\pi_n(\hat{\boldsymbol{q}}), \widehat{st}_{\hat{\text{UE}}}) = \widehat{pop}(\langle clam\rangle, \widehat{st}_{\hat{\text{UE}}})$ and, by definition, $\widehat{pop}(\langle clam\rangle, \widehat{st}_{\hat{\text{UE}}}) = (\langle clam\rangle, \widehat{st}_{\hat{\text{UE}}})$. By $\hat{\text{CEE}} \rightsquigarrow \hat{\varsigma}$, $\hat{\varsigma} = (clam', \hat{\boldsymbol{d}}, \widehat{st}, h)$ where $(\langle clam'\rangle, \widehat{st}) = \widehat{pop}(\langle CV(\hat{\text{CEE}})\rangle, \widehat{st}_{\hat{\text{CEE}}})$. By the above and Lemma 3, $\widehat{pop}(\langle CV(\hat{\text{CEE}})\rangle, \widehat{st}_{\hat{\text{CEE}}}) = (\langle clam\rangle, \widehat{st}_{\hat{\text{UE}}})$.

Lemma 5 (Single Frame). *If* $p \equiv \hat{\text{UA}} \rightsquigarrow^+ \hat{\varsigma}$, *then there exists* sm *such that, for all* $\hat{\varsigma}$, *if* $\hat{\text{UA}} = CE_p(\hat{\varsigma})$, *then* $\widehat{st}_{\hat{\varsigma}} = sm :: \widehat{st}_{\hat{\text{UA}}}$.

Proof. By induction on the definition of CE_p.

1. Path composition doesn't satisfy the premise.
2. By induction on $|p|$.
   (a) Base case of $p \equiv \hat{\text{UA}} \rightsquigarrow^0 \hat{\varsigma}' \rightsquigarrow \hat{\varsigma}$: $\hat{\text{UA}} = CE_p(\hat{\varsigma})$ holds by definition of $\rightsquigarrow$; instantiate sm thereby.
   (b) Inductive case of $p \equiv \hat{\text{UA}} \rightsquigarrow^+ \hat{\varsigma}' \rightsquigarrow \hat{\varsigma}$ where $\hat{\text{UA}} = CE_p(\hat{\varsigma}')$, $\hat{\varsigma}' \notin \widehat{UEval}$, $\hat{\varsigma}' \notin \widehat{CEvalExit}$, and $\widehat{st}_{\hat{\varsigma}'} = sm :: \widehat{st}_{\hat{\text{UA}}}$: $\widehat{st}_{\hat{\varsigma}} = sm :: \widehat{st}_{\hat{\text{UA}}}$ by cases of $\hat{\varsigma}'$ in $\hat{\varsigma}' \rightsquigarrow \hat{\varsigma}$.
3. By induction, $\widehat{st}_{\hat{\text{UE}}} = sm :: \widehat{st}_{\hat{\text{UA}}}$. By Lemma 4, $\widehat{st}_{\hat{\varsigma}} = sm :: \widehat{st}_{\hat{\text{UA}}}$.

2 Local Simulation Soundness

Lemma 6 (Local Simulation Soundness).
If $\hat{\varsigma} \rightsquigarrow \hat{\varsigma}'$ *and* $succ(|\hat{\varsigma}|_{al}) \neq \emptyset$*, then* $|\hat{\varsigma}'|_{al} \in succ(|\hat{\varsigma}|_{al})$*.*

Proof. By cases on $\hat{\varsigma}$.

The heap is simply carried over from the abstract domain and is updated in the same way in each *Apply* transition; we will not discuss it further.

1. Case $\hat{\varsigma} = ((\lambda_\gamma\,(u_1\,\ldots\,u_n\,k_1\,\ldots\,k_m)\,call), \hat{\boldsymbol{d}}, \hat{\boldsymbol{q}}, \widehat{st}, h)$:
   In the abstract, we have $\hat{\varsigma} \rightsquigarrow (call, \widehat{st}', h')$ where $\widehat{st}' = sm :: \widehat{st}$.
   Locally, we have $succ(|\hat{\varsigma}|_{al}) = succ((ulam, \hat{\boldsymbol{d}}, h)) = \{(call, h')\}$. Since $|\hat{\varsigma}'|_{al} = (call, h')$, we get $|\hat{\varsigma}'|_{al} \in \{|\hat{\varsigma}'|_{al}\}$.
2. Case $\hat{\varsigma} = ((f\,e_1\,\ldots\,e_n\,q_1\,\ldots\,q_m)_\gamma, \widehat{st}, h)$:
   In the abstract, we have $\hat{\varsigma} \rightsquigarrow (ulam, \hat{\boldsymbol{d}}, \hat{\boldsymbol{q}}', \widehat{st}', h)$ for $ulam \in \hat{\mathcal{A}}(f, h)$ where $\hat{\boldsymbol{d}} = \langle \hat{d}_1, \ldots, \hat{d}_n \rangle$ for $\hat{d}_i = \hat{\mathcal{A}}(e_i, h)$ and $(\hat{\boldsymbol{q}}', \widehat{st}')) = \widehat{pop}(\hat{\boldsymbol{q}}, \widehat{st})$ for $\hat{\boldsymbol{q}} = \langle \hat{q}_1, \ldots, \hat{q}_m \rangle$.
   Locally, we have $succ(|\hat{\varsigma}|_{al}) = succ(((f\,e_1\,\ldots\,e_n\,q_1\,\ldots\,q_m)_\gamma, h)) = \{(ulam, \hat{\boldsymbol{d}}, h) : ulam \in \mathcal{A}_u(f, \gamma)\widehat{st}h\} = \{|(ulam, \hat{\boldsymbol{d}}, \hat{\boldsymbol{q}}', \widehat{st}', h)|_{al} : ulam \in \mathcal{A}_u(f, \gamma)\widehat{st}h\}$ where $\hat{\boldsymbol{d}} = \langle \hat{d}_1, \ldots, \hat{d}_n \rangle$ for $\hat{d}_i = \mathcal{A}_u(e_i, \gamma)h$.
   The sets are identical.
3. Case $\hat{\varsigma} = ((\lambda_\gamma\,(u_1\,\ldots\,u_n)\,call), \hat{\boldsymbol{d}}, sm :: \widehat{st}, h)$:
   In the abstract, we have $\hat{\varsigma} \rightsquigarrow (call, sm :: \widehat{st}, h')$ where $\hat{\boldsymbol{d}} = \langle \hat{d}_1, \ldots, \hat{d}_n \rangle$.
   Locally, we have $succ(|\hat{\varsigma}|_{al}) = succ((clam, \hat{\boldsymbol{d}}, h)) = \{(call, h')\}$ where $\hat{\boldsymbol{d}} = \langle \hat{d}_1, \ldots, \hat{d}_n \rangle$. Since $|\hat{\varsigma}'|_{al} = (call, h')$, we get $|\hat{\varsigma}'|_{al} \in \{|\hat{\varsigma}'|_{al}\}$.
4. Case $\hat{\varsigma} = ((clam\,e_1\,\ldots\,e_n)_\gamma, \widehat{st}, h)$:
   In the abstract, we have $\hat{\varsigma} \rightsquigarrow (clam, \hat{\boldsymbol{d}}, \widehat{st}, h)$ where $\hat{\boldsymbol{d}} = \langle \hat{d}_1, \ldots, \hat{d}_n \rangle$ for $\hat{d}_i = \hat{\mathcal{A}}(e_i, h)$ since $(\langle clam \rangle, \widehat{st})) = \widehat{pop}(\langle clam \rangle, \widehat{st})$.
   Locally, we have $succ(|\hat{\varsigma}|_{al}) = succ(((clam\,e_1\,\ldots\,e_n)_\gamma, h)) = \{(clam, \hat{\boldsymbol{d}}, h)\}$ where $\hat{\boldsymbol{d}} = \langle \hat{d}_1, \ldots, \hat{d}_n \rangle$ for $\hat{d}_i = \mathcal{A}_u(e_i, \gamma)h$. Since $|\hat{\varsigma}'|_{al} = (clam, \hat{\boldsymbol{d}}, h)$, we get $|\hat{\varsigma}'|_{al} \in \{|\hat{\varsigma}'|_{al}\}$.
5. $\hat{\varsigma} = ((k\,e_1\,\ldots\,e_n)_\gamma, h)$:
   $succ(|\hat{\varsigma}|_{al}) = \emptyset$ so the premise doesn't hold.

3 Local Simulation Soundness

Lemma 7 (Local Simulation Completeness).
If $\tilde{\varsigma} \rightarrow \tilde{\varsigma}'$*, then, for each* $\hat{\varsigma}$ *such that* $\tilde{\varsigma} = |\hat{\varsigma}|_{al}$*, there exists* $\hat{\varsigma}'$ *such that* $\tilde{\varsigma}' = |\hat{\varsigma}'|_{al}$ *and* $\hat{\varsigma} \rightsquigarrow \hat{\varsigma}'$*.*

Proof. By similar arguments as the proof for local simulation soundness.

4 Path Decomposition

Lemma 8 (Path Decomposition).
All paths can be decomposed as follows:

1. *If* $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^{+} \hat{\text{CEE}}$*, then* $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^{0} \hat{\text{UA}}_1 \rightsquigarrow^{+} \hat{\text{UE}}_1 \rightsquigarrow \ldots \rightsquigarrow \hat{\text{UA}}_n \rightsquigarrow^{+} \hat{\text{UE}}_n \rightsquigarrow \hat{\text{UA}} \rightsquigarrow^{+} \hat{\text{CEE}}$ *where* $\hat{\text{UA}}_i = CE_p(\hat{\text{UE}}_i)$ *and* $\hat{\text{UA}} \equiv_p \hat{\text{CEE}}$ *by* m *for some* m *and the* m*th continuation argument of* $\hat{\text{UE}}_n$ *is some clam.*
2. *If* $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^{*} \hat{\varsigma}$ *where* $\hat{\varsigma} \notin \widehat{CEvalExit}$*, then* $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^{0} \hat{\text{UA}}_1 \rightsquigarrow^{+} \hat{\text{UE}}_1 \rightsquigarrow \ldots \rightsquigarrow \hat{\text{UA}}_n \rightsquigarrow^{+} \hat{\text{UE}}_n \rightsquigarrow \hat{\text{UA}} \rightsquigarrow^{*} \hat{\varsigma}$ *where* $\hat{\text{UA}}_i = CE_p(\hat{\text{UE}}_i)$ *and* $\hat{\text{UA}} = CE_p(\hat{\varsigma})$*.*

Proof. By induction on $|p|$.

- Base case $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^{0} \hat{\text{UA}}$: The path matches form 2 with $n = 0$. By definition of CE_p, $\hat{\mathcal{I}}(pr, =) CE_p(\hat{\text{UA}})$.
- Inductive case $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^{*} \hat{\varsigma}' \rightsquigarrow \hat{\varsigma}$: By cases on $\hat{\varsigma}$.

  1. Case $\hat{\varsigma} = \hat{\text{UA}}$: Then $\hat{\varsigma}' = \hat{\text{UE}}$ and we have $\hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^{0} \hat{\text{UA}}_1 \rightsquigarrow^{+} \hat{\text{UE}}_1 \rightsquigarrow \ldots \rightsquigarrow \hat{\text{UA}}_n \rightsquigarrow^{+} \hat{\text{UE}}_n \rightsquigarrow \hat{\text{UA}}_{n+1} \rightsquigarrow^{+} \hat{\varsigma}'$. Then for $\hat{\text{UE}}_{n+1} = \hat{\varsigma}'$, $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^{0} \hat{\text{UA}}_1 \rightsquigarrow^{+} \hat{\text{UE}}_1 \rightsquigarrow \ldots \rightsquigarrow \hat{\text{UA}}_n \rightsquigarrow^{+} \hat{\text{UE}}_n \rightsquigarrow \hat{\text{UA}}_{n+1} \rightsquigarrow^{+} \hat{\text{UE}}_{n+1} \rightsquigarrow \hat{\text{UA}} \rightsquigarrow^{*} \hat{\varsigma}$ with $\hat{\text{UA}}_{n+1} = CE_p(\hat{\text{UE}}_{n+1})$. By definition of CE_p, we have $\hat{\text{UA}} = CE_p(\hat{\varsigma})$. Thus, p matches form 2.
  2. Case $\hat{\varsigma} = \hat{\text{CA}}$: By cases on $\hat{\varsigma}'$.
     (a) Case $\hat{\varsigma}' = \hat{\text{CEI}}$: We have $\hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^{0} \hat{\text{UA}}_1 \rightsquigarrow^{+} \hat{\text{UE}}_1 \rightsquigarrow \ldots \rightsquigarrow \hat{\text{UA}}_n \rightsquigarrow^{+} \hat{\text{UE}}_n \rightsquigarrow \hat{\text{UA}} \rightsquigarrow^{+} \hat{\text{CEI}}$. By definition of CE_p, we have $\hat{\text{UA}} = CE_p(\hat{\varsigma})$. Then $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^{0} \hat{\text{UA}}_1 \rightsquigarrow^{+} \hat{\text{UE}}_1 \rightsquigarrow \ldots \rightsquigarrow \hat{\text{UA}}_n \rightsquigarrow^{+} \hat{\text{UE}}_n \rightsquigarrow \hat{\text{UA}} \rightsquigarrow^{+} \hat{\text{CA}}$. Thus, p matches form 2.
     (b) Case $\hat{\varsigma}' = \hat{\text{CEE}}$: We have $\hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^{0} \hat{\text{UA}}_1 \rightsquigarrow^{+} \hat{\text{UE}}_1 \rightsquigarrow \ldots \rightsquigarrow \hat{\text{UA}}_n \rightsquigarrow^{+} \hat{\text{UE}}_n \rightsquigarrow \hat{\text{UA}} \rightsquigarrow^{+} \hat{\text{CEE}}$. By Lemma 4, $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^{0} \hat{\text{UA}}_1 \rightsquigarrow^{+} \hat{\text{UE}}_1 \rightsquigarrow \ldots \rightsquigarrow \hat{\text{UA}}_n \rightsquigarrow^{+} \hat{\text{CA}}$ where $\hat{\text{UA}}_n = CE_p(\hat{\text{CA}})$. Thus, p matches form 2.
  3. Case $\hat{\varsigma} = \hat{\text{UE}}$: Then $\hat{\varsigma}' = \hat{\text{A}}$ and we have $\hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^{0} \hat{\text{UA}}_1 \rightsquigarrow^{+} \hat{\text{UE}}_1 \rightsquigarrow \ldots \rightsquigarrow \hat{\text{UA}}_n \rightsquigarrow^{+} \hat{\text{UE}}_n \rightsquigarrow \hat{\text{UA}} \rightsquigarrow^{*} \hat{\text{A}}$. By definition of CE_p, $\hat{\text{UA}} = CE_p(\hat{\text{E}})$. By definition of $\rightsquigarrow$, $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^{0} \hat{\text{UA}}_1 \rightsquigarrow^{+} \hat{\text{UE}}_1 \rightsquigarrow \ldots \rightsquigarrow \hat{\text{UA}}_n \rightsquigarrow^{+} \hat{\text{UE}}_n \rightsquigarrow \hat{\text{UA}} \rightsquigarrow^{+} \hat{\text{UE}}$. Thus, p matches form 2.
  4. Case $\hat{\varsigma} = \hat{\text{CEI}}$: Similar to previous case.
  5. Case $\hat{\varsigma} = \hat{\text{CEE}}$: For $m = CP(\hat{\text{UA}}, CV(\hat{\text{CEE}}))$, we have $\hat{\text{UA}} \equiv_p \hat{\text{CEE}}$ by m. By induction on n.
     (a) Base case $\hat{\text{UA}}_{i+1} \equiv_p \hat{\text{CEE}}$ by m_{i+1} and $CA(\hat{\text{UE}}_i, m) \in CLam$: Then $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^{0} \hat{\text{UA}}_1 \rightsquigarrow^{+} \hat{\text{UE}}_1 \rightsquigarrow \ldots \rightsquigarrow \hat{\text{UA}}_i \rightsquigarrow^{+} \hat{\text{UE}}_i \rightsquigarrow \hat{\text{UA}}_{i+1} \rightsquigarrow^{+} \hat{\text{CEE}}$.
     (b) Inductive case $\hat{\text{UA}}_{i+1} \equiv_p \hat{\text{CEE}}$ by m_{i+1} and $CA(\hat{\text{UE}}_i, m_{i+1}) \in CVar$: Then $\hat{\text{UA}}_i \equiv_p \hat{\text{CEE}}$ by m_i for $m_i = CP(\hat{\text{UA}}_i, m_{i+1})$.

5 Path Normalization

Definition 2 (Push Monotonicity) *A path* $p \equiv \widehat{\mathrm{UA}} \rightsquigarrow^* \hat{\varsigma}$ *is* push monotonic *if* $\widehat{st}_{\widehat{\mathrm{UA}}}$ *is a suffix of* $\widehat{st}_{\hat{\varsigma}'}$ *for each* $\hat{\varsigma}'$ *in* p.

For $p \equiv \widehat{\mathrm{UA}} \rightsquigarrow^+ \widehat{\mathrm{CEE}}$, even if $\widehat{\mathrm{UA}} \equiv_p \widehat{\mathrm{CEE}}$ by n, p isn't necessarily push monotonic: a tail call within might pop the stack below the point of entry. However, such a path can be *normalized* to remove incidental stack, and the result is push monotonic.

Definition 3 (Path Normalization) $F(p) = F_1(p, \langle\rangle)$ *for* $p \equiv \widehat{\mathrm{UA}} \rightsquigarrow^+ \widehat{\mathrm{CEE}}$ *where* $\widehat{\mathrm{UA}} \equiv_p \widehat{\mathrm{CEE}}$ *by* n

$F_1(p, \widehat{st}) = F_2(p, \widehat{st}, \widehat{st}', \langle halt, \ldots, halt\rangle)$ *where* $p \equiv \widehat{\mathrm{UA}} \rightsquigarrow^+ \widehat{\mathrm{CEE}}$ *and* $\widehat{\mathrm{UA}} = (ulam, \hat{\boldsymbol{d}}, \hat{\boldsymbol{q}}, \widehat{st}', h)$ *where* $|\hat{\boldsymbol{q}}| = |\langle halt, \ldots, halt\rangle|$

$F_2(p, \widehat{st}, \widehat{st}', \hat{\boldsymbol{q}}') = G_2(\widehat{\mathrm{UA}}, \widehat{st}, \widehat{st}', \hat{\boldsymbol{q}}') \rightsquigarrow^+ G_2(\widehat{\mathrm{CEE}}, \widehat{st}, \widehat{st}', \hat{\boldsymbol{q}}')$ *if* $\widehat{\mathrm{UA}} = CE_{\widehat{\mathrm{CEE}}}()$ *where* $p \equiv \widehat{\mathrm{UA}} \rightsquigarrow^+ \widehat{\mathrm{CEE}}$

$F_2(p, \widehat{st}, \widehat{st}', \hat{\boldsymbol{q}}') = G_2(\widehat{\mathrm{UA}}, \widehat{st}, \widehat{st}', \hat{\boldsymbol{q}}') \rightsquigarrow^+ G_2(\widehat{\mathrm{UE}}, \widehat{st}, \widehat{st}', \hat{\boldsymbol{q}}') \rightsquigarrow F_3(p', \widehat{st}, \widehat{st}', \hat{\boldsymbol{q}}')$ *if* $\widehat{\mathrm{UA}} = CE_{\widehat{\mathrm{UE}}}()$ *where* $p \equiv \widehat{\mathrm{UA}} \rightsquigarrow^+ \widehat{\mathrm{UE}} \rightsquigarrow p'$ *and* $p' \equiv \widehat{\mathrm{UA}}_0 \rightsquigarrow^+ \widehat{\mathrm{CEE}}$ *where* $\widehat{\mathrm{UA}}_0 \equiv_p \widehat{\mathrm{CEE}}$ *by* n_0

$F_3(p, \widehat{st}, \widehat{st}', \hat{\boldsymbol{q}}) = F_2(p, \widehat{st}, \widehat{st}', \hat{\boldsymbol{q}})$ *if* $\widehat{st}'$ *is a suffix of* $\widehat{st}_{\widehat{\mathrm{UA}}}$ *where* $p \equiv \widehat{\mathrm{UA}} \rightsquigarrow^+ \widehat{\mathrm{CEE}}$

$F_3(p, \widehat{st}, \widehat{st}', \hat{\boldsymbol{q}}) = F_1(p, \langle\rangle)$ *if* $\widehat{st}'$ *is not a suffix of* $\widehat{st}_{\widehat{\mathrm{UA}}}$ *where* $p \equiv \widehat{\mathrm{UA}} \rightsquigarrow^+ \widehat{\mathrm{CEE}}$

$G_2((ulam, \hat{\boldsymbol{d}}, \hat{\boldsymbol{q}}, \widehat{st}, h), \widehat{st}, \widehat{st}', \hat{\boldsymbol{q}}') = (ulam, \hat{\boldsymbol{d}}, \hat{\boldsymbol{q}}', \widehat{st}', h)$

$G_2((\ldots, \widehat{st}_0, h), \widehat{st}, \widehat{st}', \hat{\boldsymbol{q}}') = (\ldots, \widehat{st}'', h)$

$\widehat{st}'' = fr_1 :: \cdots :: fr_n :: fr'' :: \widehat{st}'$

$fr'' = sm''$

$sm'' = [k_1 \mapsto \hat{q}_1', \ldots, k_m \mapsto \hat{q}_m']$

$\hat{\boldsymbol{q}}' = \langle \hat{q}_1', \ldots, \hat{q}_m' \rangle$

$sm = [k_1 \mapsto \hat{q}_1, \ldots, k_m \mapsto \hat{q}_m]$

$fr = sm$

$\widehat{st}_0 = fr_1 :: \cdots :: fr_n :: fr :: \widehat{st}$

Lemma 9 (Stack Irrelevance).

If $p \equiv \widehat{\mathrm{UA}} \rightsquigarrow^+ \widehat{\mathrm{CEE}}$ *where* $\widehat{\mathrm{UA}} = (ulam, \hat{\boldsymbol{d}}, \hat{\boldsymbol{q}}, \widehat{st}, h)$, $\widehat{\mathrm{UA}} \equiv_p \widehat{\mathrm{CEE}}$ *by* n, *and* $\widehat{pop}(\langle \pi_n(\hat{\boldsymbol{q}})\rangle, \widehat{st}) = (\langle cp\rangle, \widehat{st}')$, *then, for any stack* $\widehat{st}''$, $F_{\widehat{\mathrm{UA}}}\widehat{st}'\widehat{st}'' \equiv_p F_{\widehat{\mathrm{CEE}}}\widehat{st}'\widehat{st}''$ *by* n.

Proof. After application of Definition 3, by induction on $\cdot \equiv_p \cdot$ by $\cdot$.

6 Summarization Soundness

We prove that summarization is sound by induction on path length. In the inductive step, we discriminate the penultimate state in the path. By the quasi-completeness of the local semantics and the explicit handling of returns by the algorithm, every possible ultimate state of the path is considered.

Theorem 2 (Summarization Soundness).
After summarization,

1. *if* $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^* \hat{\text{UA}} \rightsquigarrow^* \hat{\varsigma}$ *such that* $\hat{\text{UA}} = CE_{\hat{\varsigma}}()$*,* $(|\hat{\text{UA}}|_{al}, |\hat{\varsigma}|_{al}) \in Seen$*;*
2. *if* $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^* \hat{\text{UA}} \rightsquigarrow^+ \hat{\text{CEE}}$ *such that* $\hat{\text{UA}} \equiv_p \hat{\text{CEE}}$ *by* n*, then* $(|\hat{\text{UA}}|_{al}, |\hat{\text{CEE}}|_{al}, n) \in$ *Summary; and*
3. *if* $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^+ \hat{\varsigma}$ *such that* $\hat{\varsigma}$ *is a final state, then* $|\hat{\varsigma}|_{al} \in Final$*.*

Proof. By induction on $|p|$.
Base case $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^0 \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}})$:
At summarization commencement, $(\tilde{\mathcal{I}}(pr,,)\tilde{\mathcal{I}}(pr,)) \in Seen$.
Inductive case $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^* \hat{\varsigma} \rightsquigarrow \hat{\varsigma}'$:
By cases on $\hat{\varsigma}$.

1. Case $\hat{\varsigma} = \hat{\text{UA}}$: By induction, $(|\hat{\varsigma}|_{al}, |\hat{\varsigma}|_{al})$ is added to *Work*, since $\hat{\varsigma} = CE_{\hat{\varsigma}}()$. By Lemma 7, the first case of the main loop calls `Propagate`$(|\hat{\text{UA}}|_{al}, |\hat{\varsigma}'|_{al})$. The result follows from the soundness of `Propagate`.
2. Case $\hat{\varsigma} = \hat{\text{CA}}$ or $\hat{\varsigma} = \hat{\text{CEI}}$: By induction, $(|\hat{\text{UA}}|_{al}, |\hat{\varsigma}|_{al})$ is added to *Work*, where $\hat{\text{UA}} = CE_{\hat{\varsigma}}()$. By Lemma 7, the first case of the main loop calls `Propagate`$(|\hat{\text{UA}}|_{al}, |\hat{\varsigma}'|_{al})$. The result follows from the soundness of `Propagate`.
3. Case $\hat{\varsigma} = \hat{\text{UE}}$:
By induction, $(|\hat{\text{UA}}_0|_{al}, |\hat{\varsigma}|_{al})$ is added to *Work*, where $\hat{\text{UA}}_0 = CE_{\hat{\varsigma}}()$. By Lemma 7, the second case of the main loop calls `Propagate`$(|\hat{\varsigma}'|_{al}, |\hat{\varsigma}'|_{al})$, since $\hat{\varsigma}' = CE_{\hat{\varsigma}'}()$. If a summary exists, then it holds by Lemma 9. If a summary doesn't exist, then it holds by Lemma 4.
4. Case $\hat{\varsigma} = \hat{\text{CEE}}$: By induction, $(|\hat{\text{UA}}|_{al}, |\hat{\varsigma}|_{al})$ is added to *Work*, where $\hat{\text{UA}} = CE_{\hat{\varsigma}}()$. The third case of the main loop calls `Return`$(|\hat{\text{UA}}|_{al}, |\hat{\text{UA}}|_{al}, CP(|\hat{\text{UA}}|_{al}, CV(|\hat{\varsigma}|_{al})))$. The result follows by the soundness of `Return`.

Lemma 10 (`Return` Sound).
If

1. $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \rightsquigarrow^0 \hat{\text{UA}}_1 \rightsquigarrow^+ \hat{\text{UE}}_1 \rightsquigarrow \ldots \rightsquigarrow \hat{\text{UA}}_n \rightsquigarrow^+ \hat{\text{UE}}_n \rightsquigarrow \hat{\text{UA}} \rightsquigarrow^+ \hat{\text{CEE}}$ *such that* $\hat{\text{UA}}_i = CE_{\hat{\text{UE}}_i}()$*;*
2. $\hat{\text{UA}} \equiv_p \hat{\text{CEE}}$ *by* j*;*
3. $(|\hat{\text{UA}}_i|_{al}, |\hat{\text{UE}}_i|_{al}, |\hat{\text{UA}}_{i+1}|_{al}) \in Call$*;*
4. $(|\hat{\text{UA}}_n|_{al}, |\hat{\text{UE}}_n|_{al}, |\hat{\text{UA}}|_{al}) \in Call$*; and*
5. *if* $(|\hat{\text{UA}}|_{al}, |\hat{\text{CEE}}|_{al}, j) \in Summary$*, then*
   (a) *if* $\hat{\text{UA}}_i \equiv_p \hat{\text{CEE}}$ *by* j_i*, then* $(|\hat{\text{UA}}_i|_{al}, |\hat{\text{CEE}}|_{al}, j_i) \in Summary$*; and*
   (b) *if* $\hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \equiv_p \hat{\text{CEE}}$ *by* 1 *and* $\hat{\text{CEE}} \rightsquigarrow \hat{\varsigma}$*, then* $|\hat{\varsigma}|_{al} \in Final$*.*

then, after ***Return***$(|\hat{\text{UA}}|_{al}, |\hat{\text{CEE}}|_{al}, j)$*,*

1. $(|\hat{\text{UA}}|_{al}, |\hat{\text{CEE}}|_{al}, j) \in Summary$*;*
2. *if* $\hat{\text{UA}}_i \equiv_p \hat{\text{CEE}}$ *by* j_i*, then* $(|\hat{\text{UA}}_i|_{al}, |\hat{\text{CEE}}|_{al}, j_i) \in Summary$*; and*
3. *if* $\hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \equiv_p \hat{\text{CEE}}$ *by* 1 *and* $\hat{\text{CEE}} \rightsquigarrow \hat{\varsigma}$*, then* $|\hat{\varsigma}|_{al} \in Final$*.*

Proof. By case analysis on *Summary* and induction on Lemma 11.

Lemma 11 (`Link` **Sound).**
If

1. $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \leadsto^0 \widehat{\text{UA}}_1 \leadsto^+ \widehat{\text{UE}}_1 \leadsto \ldots \leadsto \widehat{\text{UA}}_n \leadsto^+ \widehat{\text{UE}}_n \leadsto \widehat{\text{UA}} \leadsto^+ \widehat{\text{CEE}}$ *such that* $\widehat{\text{UA}}_i = CE_{\widehat{\text{UE}}_i}()$*;*
2. $\widehat{\text{UA}} \equiv_p \widehat{\text{CEE}}$ *by* j*;*
3. $(|\widehat{\text{UA}}_i|_{al}, |\widehat{\text{UE}}_i|_{al}, |\widehat{\text{UA}}_{i+1}|_{al}) \in \mathit{Call}$*;*
4. $(|\widehat{\text{UA}}_n|_{al}, |\widehat{\text{UE}}_n|_{al}, |\widehat{\text{UA}}|_{al}) \in \mathit{Call}$*; and*
5. $(|\widehat{\text{UA}}|_{al}, |\widehat{\text{CEE}}|_{al}, j) \in \mathit{Summary}$*.*

then, after $\textit{\textbf{Link}}(|\widehat{\text{UA}}_n|_{al}, |\widehat{\text{UE}}_n|_{al}, |\widehat{\text{UA}}|_{al}, |\widehat{\text{CEE}}|_{al}, j)$*,*

1. *if* $CA(|\widehat{\text{UE}}_n|_{al}, j) = k$*, then preconditions for* $\textit{\textbf{Return}}(|\widehat{\text{UA}}_n|_{al}, |\widehat{\text{CEE}}|_{al}, CP(|\widehat{\text{UA}}_n|_{al}, k))$ *are met and its postconditions hold; and*
2. *if* $CA(|\widehat{\text{UE}}_n|_{al}, j) = \mathit{clam}$*, then preconditions for* $\textit{\textbf{Update}}(|\widehat{\text{UA}}_n|_{al}, |\widehat{\text{UA}}|_{al}, |\widehat{\text{UE}}_n|_{al})|\widehat{\text{CEE}}|_{al}j$ *are met and its postconditions hold.*

Proof. By cases on $CA(|\widehat{\text{UE}}_n|_{al}, j)$, induction on Lemma 10, and Lemma 12.

Lemma 12 (`Update` **Sound).**
If

1. $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \leadsto^0 \widehat{\text{UA}}_1 \leadsto^+ \widehat{\text{UE}}_1 \leadsto \ldots \leadsto \widehat{\text{UA}}_n \leadsto^+ \widehat{\text{UE}}_n \leadsto \widehat{\text{UA}} \leadsto^+ \widehat{\text{UE}} \leadsto \widehat{\text{UA}}' \leadsto^+ \widehat{\text{CEE}}$ *such that* $\widehat{\text{UA}}_i = CE_{\widehat{\text{UE}}_i}()$ *and* $\widehat{\text{UA}} = CE_{\widehat{\text{UE}}}()$*;*
2. $\widehat{\text{UA}}' \equiv_p \widehat{\text{CEE}}$ *by* j*;*
3. $(|\widehat{\text{UA}}'|_{al}, |\widehat{\text{CEE}}|_{al}, j) \in \mathit{Summary}$*;*
4. $(|\widehat{\text{UA}}_i|_{al}, |\widehat{\text{UE}}_i|_{al}, |\widehat{\text{UA}}_{i+1}|_{al}) \in \mathit{Call}$*;*
5. $(|\widehat{\text{UA}}_n|_{al}, |\widehat{\text{UE}}_n|_{al}, |\widehat{\text{UA}}|_{al}) \in \mathit{Call}$*;*
6. $(|\widehat{\text{UA}}|_{al}, |\widehat{\text{UE}}|_{al}, |\widehat{\text{UA}}'|_{al}) \in \mathit{Call}$*; and*
7. $CA(|\widehat{\text{UE}}|_{al}, j) = \mathit{clam}$

then, after $\textit{\textbf{Link}}(|\widehat{\text{UA}}|_{al}, |\widehat{\text{UE}}|_{al}, |\widehat{\text{UA}}'|_{al}, |\widehat{\text{CEE}}|_{al}, j)$*, the postconditions of* $\textit{\textbf{Propagate}}(|\widehat{\text{UA}}|_{al}, |\hat{\varsigma}|_{al})$ *hold, where* $\widehat{\text{CEE}} \leadsto \hat{\varsigma}$*.*

Proof. By Lemma 4, Lemma 3, and the definition of $CE_{\cdot}$.

Lemma 13 (`Final` **Sound).**
If $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \leadsto^+ \widehat{\text{CEE}}$ *such that* $\hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \equiv_p \widehat{\text{CEE}}$ *by* 1*, then, after* $\textit{\textbf{Final}}(|\widehat{\text{CEE}}|_{al})$*,* $|\hat{\varsigma}|_{al} \in \mathit{Final}$*, where* $\widehat{\text{CEE}} \leadsto \hat{\varsigma}$*.*

Proof. By Lemma 3.

7 Summarization Soundness

Theorem 3 (Summarization Completeness).
After summarization,

1. *if* $(\widetilde{\text{UA}}, \tilde{\varsigma}) \in \mathit{Seen}$*, then there exists* $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \leadsto^* \widehat{\text{UA}} \leadsto^* \hat{\varsigma}$ *such that* $\widetilde{\text{UA}} = |\widehat{\text{UA}}|_{al}$*,* $\tilde{\varsigma} = |\hat{\varsigma}|_{al}$*, and* $\widehat{\text{UA}} = CE_{\hat{\varsigma}}()$*;*

2. *if* $(\widetilde{\text{UA}}, \widetilde{\text{CEE}}, n) \in \mathit{Summary}$ *then there exists* $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \leadsto^* \widehat{\text{UA}} \leadsto^+ \widehat{\text{CEE}}$ *such that* $\widetilde{\text{UA}} = |\widehat{\text{UA}}|_{al}$*,* $\widetilde{\text{CEE}} = |\widehat{\text{CEE}}|_{al}$*, and* $\widehat{\text{UA}} \equiv_p \widehat{\text{CEE}}$ *by* n*; and*
3. *if* $\tilde{\varsigma} \in \mathit{Final}$*, then there exists* $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \leadsto^+ \hat{\varsigma}$ *such that* $\tilde{\varsigma} = |\hat{\varsigma}|_{al}$ *and* $\hat{\varsigma}$ *is a final state.*

Proof. By induction on the number of iterations n through the loop.

Base case $n = 0$:

At summarization commencement, $(\tilde{\mathcal{I}}(pr,,)\tilde{\mathcal{I}}(pr,)) \in \mathit{Seen}$ and $\hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \leadsto \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}})$.

Inductive case $n = i$:

Each iteration commences by considering $(\widetilde{\text{UA}}, \tilde{\varsigma})$ such that there is a path $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \leadsto^* \widehat{\text{UA}} \leadsto^* \hat{\varsigma}$ such that $\widetilde{\text{UA}} = |\widehat{\text{UA}}|_{al}$ and $\tilde{\varsigma} = |\hat{\varsigma}|_{al}$.

By cases on $\tilde{\varsigma}$.

1. Case $\tilde{\varsigma} = \widetilde{\text{UA}}$ or $\tilde{\varsigma} = \widetilde{\text{CA}}$ or $\tilde{\varsigma} = \widetilde{\text{CEI}}$:
   The first case of the main loop calls `Propagate`$(\widetilde{\text{UA}}, \tilde{\varsigma}')$ for each $\tilde{\varsigma}' \in \mathit{succ}(\tilde{\varsigma})$. By Lemma 7, there exists $\hat{\varsigma}'$ such that $\hat{\varsigma} \leadsto \hat{\varsigma}'$ and $|\hat{\varsigma}'|_{al} = \tilde{\varsigma}'$. Then there exists path $\hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \leadsto^* \widehat{\text{UA}} \leadsto^* \hat{\varsigma} \leadsto \hat{\varsigma}'$.
2. Case $\tilde{\varsigma} = \widetilde{\text{UE}}$:
   By Lemma 7, for each $\tilde{\varsigma}' \in \mathit{succ}(\tilde{\varsigma})$, there is $\hat{\varsigma}'$ such that $\hat{\varsigma} \leadsto \hat{\varsigma}'$ and $|\hat{\varsigma}'|_{al} = \tilde{\varsigma}'$. Then there exists path $\hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \leadsto^* \widehat{\text{UA}} \leadsto^* \hat{\varsigma} \leadsto \hat{\varsigma}'$ and the preconditions for `Propagate`$(\tilde{\varsigma}', \tilde{\varsigma}')$ are met. Suppose $(\tilde{\varsigma}', \widetilde{\text{CEE}}, j) \in \mathit{Summary}$. By Lemma 9, there exists path $\hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \leadsto^* \widehat{\text{UA}} \leadsto^+ \hat{\varsigma} \leadsto \hat{\varsigma}' \leadsto^+ \widehat{\text{CEE}}$ such that $|\widehat{\text{CEE}}|_{al} = \widetilde{\text{CEE}}$ and $\hat{\varsigma}' \equiv_p \widehat{\text{CEE}}$ by j. With $(\widetilde{\text{UA}}, \tilde{\varsigma}, \tilde{\varsigma}') \in \mathit{Call}$, the preconditions for `Link`$(\widetilde{\text{UA}}, \tilde{\varsigma}, \tilde{\varsigma}', \widetilde{\text{CEE}}, j)$ are met and its postconditions hold.
3. Case $\tilde{\varsigma} = \widetilde{\text{CEE}}$:
   By definition, $\widehat{\text{UA}} \equiv_p \hat{\varsigma}$ by $\mathit{CP}(\widehat{\text{UA}}, \mathit{CV}(\hat{\varsigma}))$. Then the preconditions for `Return`$(\widetilde{\text{UA}}, \tilde{\varsigma}, \mathit{CP}(\widetilde{\text{UA}}, \mathit{CV}(\tilde{\varsigma})))$ are met and its postconditions hold.

Lemma 14 (`Return` Complete).

If

1. *there exists* $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \leadsto^0 \widehat{\text{UA}}_1 \leadsto^+ \widehat{\text{UE}}_1 \leadsto \ldots \leadsto \widehat{\text{UA}}_n \leadsto^+ \widehat{\text{UE}}_n \leadsto \widehat{\text{UA}} \leadsto^+ \widehat{\text{CEE}}$ *such that* $\widehat{\text{UA}}_i = \mathit{CE}_{\widehat{\text{UE}}_i}()$*;*
2. $\widehat{\text{UA}} \equiv_p \widehat{\text{CEE}}$ *by* j*;*
3. $(|\widehat{\text{UA}}_i|_{al}, |\widehat{\text{UE}}_i|_{al}, |\widehat{\text{UA}}_{i+1}|_{al}) \in \mathit{Call}$*;*
4. $(|\widehat{\text{UA}}_n|_{al}, |\widehat{\text{UE}}_n|_{al}, |\widehat{\text{UA}}|_{al}) \in \mathit{Call}$*; and*

then, after ***`Return`***$(|\widehat{\text{UA}}|_{al}, |\widehat{\text{CEE}}|_{al}, j)$*,*

1. *if* $(|\widehat{\text{UA}}_i|_{al}, |\widehat{\text{CEE}}|_{al}, j_i) \in \mathit{Summary}$*, then there exists path with* $\widehat{\text{UA}}_i \equiv_p \widehat{\text{CEE}}$ *by* j_i*; and*
2. *if* $|\hat{\varsigma}|_{al} \in \mathit{Final}$*, then there exists path with* $\hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \equiv_p \widehat{\text{CEE}}$ *by* 1 *and* $\widehat{\text{CEE}} \leadsto \hat{\varsigma}$*.*

Proof. By Lemma 5 and Lemma 3.

Lemma 15 (`Link` Complete).

If

1. *there exists path* $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \leadsto^* \widehat{\mathrm{UA}} \leadsto^+ \widehat{\mathrm{UE}} \leadsto \widehat{\mathrm{UA}}^* \leadsto^+ \widehat{\mathrm{CEE}}$ *such that* $\widehat{\mathrm{UA}}_i = CE_{\widehat{\mathrm{UE}}_i}()$;
2. $\widehat{\mathrm{UA}} \equiv_p \widehat{\mathrm{CEE}}$ *by* j;
3. $(|\widehat{\mathrm{UA}}_i|_{al}, |\widehat{\mathrm{UE}}_i|_{al}, |\widehat{\mathrm{UA}}_{i+1}|_{al}) \in$ *Call;*
4. $(|\widehat{\mathrm{UA}}_n|_{al}, |\widehat{\mathrm{UE}}_n|_{al}, |\widehat{\mathrm{UA}}|_{al}) \in$ *Call; and*
5. $(|\widehat{\mathrm{UA}}|_{al}, |\widehat{\mathrm{CEE}}|_{al}, j) \in$ *Summary.*

then, after ***Link***$(|\widehat{\mathrm{UA}}_n|_{al}, |\widehat{\mathrm{UE}}_n|_{al}, |\widehat{\mathrm{UA}}|_{al}, |\widehat{\mathrm{CEE}}|_{al}, j)$,

1. *if* $CA(|\widehat{\mathrm{UE}}_n|_{al}, j) = k$, *then preconditions for* ***Return***$(|\widehat{\mathrm{UA}}_n|_{al}, |\widehat{\mathrm{CEE}}|_{al}, CP(|\widehat{\mathrm{UA}}_n|_{al}, k))$ *are met and its postconditions hold; and*
2. *if* $CA(|\widehat{\mathrm{UE}}_n|_{al}, j) = clam$, *then preconditions for* ***Update***$(|\widehat{\mathrm{UA}}_n|_{al}, |\widehat{\mathrm{UA}}|_{al}, |\widehat{\mathrm{UE}}_n|_{al})|\widehat{\mathrm{CEE}}|_{al} j$ *are met and its postconditions hold.*

Proof. By cases on $CA(|\widehat{\mathrm{UE}}_n|_{al}, j)$, induction on Lemma 14, and Lemma 16.

Lemma 16 **(**`Update` **Complete).**
If there exists path $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \leadsto^* \widehat{\mathrm{UA}} \leadsto^+ \widehat{\mathrm{UE}} \leadsto \widehat{\mathrm{UA}}^* \leadsto^+ \widehat{\mathrm{CEE}}$ *such that* $\widehat{\mathrm{UA}}^* \equiv_p \widehat{\mathrm{CEE}}$ *by* j *and* $CA(\widehat{\mathrm{UE}}, j) = clam$, *then, after* ***Update***$(\widetilde{\mathrm{UA}}, \widetilde{\mathrm{UA}}^*, \widetilde{\mathrm{UE}})\widetilde{\mathrm{CEE}} j$ *such that* $|\widehat{\mathrm{UA}}|_{al} = \widetilde{\mathrm{UA}}$, $|\widehat{\mathrm{UE}}|_{al} = \widetilde{\mathrm{UE}}$, $|\widehat{\mathrm{UA}}^*|_{al} = \widetilde{\mathrm{UA}}^*$, *and* $|\widehat{\mathrm{CEE}}|_{al} = \widetilde{\mathrm{CEE}}$, $(\widetilde{\mathrm{UA}}, \tilde{\varsigma}) \in$ *Seen and there exists* $p' \equiv p \leadsto \hat{\varsigma}$ *such that* $\tilde{\varsigma} = |\hat{\varsigma}|_{al}$.

Proof. By Lemma 4 and Lemma 9.

Lemma 17 **(**`Final` **Complete).**
If, for $\widetilde{\mathrm{CEE}}$, *there exists path* $p \equiv \hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \leadsto^+ \widehat{\mathrm{CEE}}$ *such that* $\hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \equiv_p \widehat{\mathrm{CEE}}$ *by* 1 *and* $|\widehat{\mathrm{CEE}}|_{al} = \widetilde{\mathrm{CEE}}$, *then, after* ***Final***$(\widetilde{\mathrm{CEE}})$, $\tilde{\varsigma} \in$ *Final and* $\hat{\mathcal{I}}(pr, \hat{\boldsymbol{d}}) \leadsto^+ \widehat{\mathrm{CEE}} \leadsto \hat{\varsigma}$ *where* $|\hat{\varsigma}|_{al} = \tilde{\varsigma}$.

Proof. By Lemma 3.