École normale supérieure, MPRI, M2 **Year 2007/2008**

Course 2-6 "Abstract interpretation: application to verification and static analysis"

P. Cousot

Questions and answers of the partial exam of Friday November 23th, 2007, 8:45–11:45

The questions can be considered in any order (assuming the results of the previous ones). The grade of each question will be marked independently of the others. If a question is ambiguous or even erroneous, it is part of the question to solve the ambiguity or error. The difficulty of each question is estimated by one star for the easiest and three stars for the more difficult ones. Course handout and personnal notes are the only authorized documents.

1. Traces

Given a set $\mathcal{S}$, we let $\mathcal{S}^\star$ be the set of finite sequences over the set $\mathcal{S}$ including the empty sequence ϵ, $\mathcal{S}^+ \triangleq \mathcal{S}^\star \setminus \{\epsilon\}$, $\mathcal{S}^\omega$ be the set of infinite sequences over $\mathcal{S}$, $\mathcal{S}^\infty \triangleq \mathcal{S}^\star \cup \mathcal{S}^\omega$ be the set of finite or infinite sequences over $\mathcal{S}^1$, and $\mathcal{S}^\infty \triangleq \mathcal{S}^+ \cup \mathcal{S}^\omega$ be the set of nonempty finite or infinite sequences over $\mathcal{S}$. We let $|\sigma| \in \mathbb{N} \cup \{\omega\}$ be the length of $\sigma \in \mathcal{S}^\infty$, in particular $|\epsilon| = 0$ and $\mathcal{S}^n \triangleq \{\sigma \in \mathcal{S}^\star \mid |\sigma| = n\}$. We let $\bullet$ be the concatenation of traces so that $\epsilon \bullet \sigma = \sigma \bullet \epsilon = \sigma$ and $\sigma \bullet \varsigma = \sigma$ when $\sigma \in \mathcal{S}^\omega$. If $\sigma \in \mathcal{S}^+$ then $|\sigma| > 0$ and $\sigma = \sigma_0 \bullet \sigma_1 \bullet \ldots \bullet \sigma_{|\sigma|-1}$. If $\sigma \in \mathcal{S}^\omega$ then $|\sigma| = \omega$ and $\sigma = \sigma_0 \bullet \sigma_1 \bullet \ldots \bullet \sigma_n \bullet \ldots$.

Given $X, Y \in \wp(\mathcal{S}^\infty)$, we define $X^+ \triangleq X \cap \mathcal{S}^+$, $X^\omega \triangleq X \cap \mathcal{S}^\omega$ and $X \sqsubseteq Y \triangleq X^+ \subseteq Y^+ \wedge X^\omega \supseteq Y^\omega$.

Question 1.1 ($\star$) *Prove that $\langle \wp(\mathcal{S}^\infty), \sqsubseteq \rangle$ is a complete lattice (and provide the infimum, supremum, least upper bound (lub) $\sqcup$ and greatest lower bound (glb) $\sqcap$).*

Answer to question 1.1

See the course, we have $\bigsqcup_{i \in \Delta} X_i = \bigcup_{i \in \Delta} X_i^+ \cup \bigcap_{i \in \Delta} X_i^\omega$. □

2. Trace semantics of the eager λ-calculus

2.1 Syntax

The syntax of the λ-calculus with constants is

[1] The "proportional to" symbol $\propto$ is used as a pictogram similar to "infinity" ∞ but with the possibility of emptyness.

$$
\begin{array}{rcll}
\mathsf{x}, \mathsf{y}, \mathsf{z}, \ldots & \in & \mathbb{X} & \text{variables} \\
\mathsf{c} & \in & \mathbb{C} & \text{constants } (\mathbb{X} \cap \mathbb{C} = \varnothing) \\
\mathsf{c} & ::= & 0 \mid 1 \mid \ldots & \\
\mathsf{v} & \in & \mathbb{V} & \text{values} \\
\mathsf{v} & ::= & \mathsf{c} \mid \boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{a} & \\
\mathsf{e} & \in & \mathbb{E} & \text{errors} \\
\mathsf{e} & ::= & \mathsf{c}\ \mathsf{a} \mid \mathsf{e}\ \mathsf{a} & \\
\mathsf{a}, \mathsf{a}', \mathsf{a}_1, \ldots, \mathsf{b}, , \ldots & \in & \mathbb{T} & \text{terms} \\
\mathsf{a} & ::= & \mathsf{x} \mid \mathsf{v} \mid \mathsf{a}\ \mathsf{a}' &
\end{array}
$$

We write $\mathsf{a}[\mathsf{x} \leftarrow \mathsf{b}]$ for the capture-avoiding substitution of b for all free occurences of x within a. We let $\mathrm{FV}(\mathsf{a})$ be the free variables of a.

2.2 Trace semantics

We define the call-by-value semantics of closed terms (without free variables) $\overline{\mathbb{T}} \triangleq \{\mathsf{a} \in \mathbb{T} \mid \mathrm{FV}(\mathsf{a}) = \varnothing\}$.

The application $(\boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{a})\ \mathsf{v}$ of a function $\boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{a}$ to a value v is evaluated by substitution $\mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}]$ of the actual parameter v for the formal parameter x in the function body a. This cannot be understood as induction on the program syntax since $\mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}]$ is not in general a strict syntactic subcomponent of $(\boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{a})\ \mathsf{v}$. Recursion will be handled using fixpoints in the complete lattice $\langle \wp(\mathbb{T}^\infty), \sqsubseteq \rangle$ of traces defined in Question 1.1.

For $\mathsf{a} \in \mathbb{T}$ and $\sigma \in \mathbb{T}^\infty$, we define the application $\mathsf{a}@\sigma$ of a term a to a trace σ to be $\sigma' \in \mathbb{T}^\infty$ such that $\forall i < |\sigma| : \sigma'_i = \mathsf{a}\ \sigma_i$ and similarly the application $\sigma@\mathsf{a}$ of a trace σ to a term a to be σ' such that $\forall i < |\sigma| : \sigma'_i = \sigma_i\ \mathsf{a}$.

The bifinitary trace semantics $\vec{\mathbb{S}} \in \wp(\overline{\mathbb{T}}^\infty)$ of the closed call-by-value λ-calculus $\overline{\mathbb{T}}$ can be specified in fixpoint form $\vec{\mathbb{S}} = \mathbf{lfp}^{\sqsubseteq} \vec{F}$ where the set of traces transformer $\vec{F} \in \wp(\overline{\mathbb{T}}^\infty) \longrightarrow \wp(\overline{\mathbb{T}}^\infty)$ describes big steps of computation

$$
\begin{array}{rcll}
\vec{F}(S) & \triangleq & \{\mathsf{v} \in \overline{\mathbb{T}}^\infty \mid \mathsf{v} \in \mathbb{V}\} \cup & \text{(a)} \\
& & \{(\boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{a})\ \mathsf{v} \bullet \mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}] \bullet \sigma \mid \mathsf{v} \in \mathbb{V} \wedge \mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}] \bullet \sigma \in S\} \cup & \text{(b)} \\
& & \{\sigma@\mathsf{b} \mid \sigma \in S^\omega\} \cup & \text{(c)} \\
& & \{(\sigma@\mathsf{b}) \bullet (\mathsf{v}\ \mathsf{b}) \bullet \sigma' \mid \sigma \neq \epsilon \wedge \sigma \bullet \mathsf{v} \in S^+ \wedge \mathsf{v} \in \mathbb{V} \wedge (\mathsf{v}\ \mathsf{b}) \bullet \sigma' \in S\} \cup & \text{(d)} \\
& & \{\mathsf{a}@\sigma \mid \mathsf{a} \in \mathbb{V} \wedge \sigma \in S^\omega\} \cup & \text{(e)} \\
& & \{(\mathsf{a}@\sigma) \bullet (\mathsf{a}\ \mathsf{v}) \bullet \sigma' \mid \mathsf{a}, \mathsf{v} \in \mathbb{V} \wedge \sigma \neq \epsilon \wedge \sigma \bullet \mathsf{v} \in S^+ \wedge (\mathsf{a}\ \mathsf{v}) \bullet \sigma' \in S\}\ . & \text{(f)}
\end{array}
$$

The definition of $\vec{F}$ has (a) for termination, (b) for call-by-value β-reduction, (c) and (d) for left reduction under applications and (e) and (f) for right reduction under applications, corresponding to left-to-right evaluation. (b), (d) and (f) cope both with terminating and diverging traces.

Question 2.1 ($\star\star$) *Prove that $\vec{F}$ is $\subseteq$-monotone but not $\sqsubseteq$-monotone (e.g. using the term $\theta\ \theta$ where $\theta \triangleq \boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{x}\ \mathsf{x}$).*

Answer to question 2.1

$\subseteq$-monotony holds for (a) and $\cup$ and can be proved for all cases (b)–(f) of the form $F(S) = \{f(\mathsf{a}, \mathsf{a}', ..., \sigma, \sigma') \mid p(\mathsf{a}, \mathsf{a}', ...) \wedge g(\sigma) \in S^+ \wedge h(\sigma') \in S\}$ so that $S \subseteq S'$ implies $F(S) \subseteq F(S')$.

For a counter-example to $\sqsubseteq$-monotony, define $X^+ \triangleq X \cap \mathbb{T}^+$, $X^\omega \triangleq X \cap \mathbb{T}^\omega$ and consider $\theta \triangleq \boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{x}\,\mathsf{x}$, $X = \{(\theta\ \theta)^\omega\}$ (where $\mathsf{a}^\omega \triangleq \mathsf{a} \bullet \mathsf{a} \bullet \mathsf{a} \bullet ...$) and $Y = \{(\boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{x}\ \theta) \bullet \theta,\ (\theta\ \theta)^\omega\}$. We have $X \sqsubseteq Y$ since $X^+ = \varnothing \subseteq \{(\boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{x}\ \theta) \bullet \theta\} = Y^+$ and $X^\omega = \{(\theta\ \theta)^\omega\} \supseteq \{(\theta\ \theta)^\omega\} = Y^\omega$. However $\vec{F}(X) \not\sqsubseteq \vec{F}(Y)$. Indeed by (d), we have $((\boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{x}\ \theta)\ \theta) \bullet (\theta\ \theta) \bullet (\theta\ \theta)^\omega = ((\boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{x}\ \theta)\ \theta) \bullet (\theta\ \theta)^\omega \in \vec{F}(Y)$ while $((\boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{x}\ \theta)\ \theta) \bullet (\theta\ \theta)^\omega \notin \vec{F}(X)$ by examining all cases (a)—(f). □

Recall that $S^+ \triangleq S \cap \mathbb{T}^+$, $S^\omega \triangleq S \cap \mathbb{T}^\omega$ so $S^+ \cap S^\omega = \varnothing$ and define

$$\vec{\mathbb{S}}^+ \quad \triangleq \quad \mathbf{lfp}^{\subseteq}\, \vec{F}^+ \quad \text{where} \quad \vec{F}^+(S) \quad \triangleq \quad (\vec{F}(S^+))^+ \ .$$

Define

$$\vec{\mathbb{S}}^\omega \quad \triangleq \quad \mathbf{gfp}^{\subseteq}\, \vec{F}^\omega \quad \text{where} \quad \vec{F}^\omega(S) \quad \triangleq \quad (\vec{F}(\vec{\mathbb{S}}^+ \cup S^\omega))^\omega \ .$$

Question 2.2 ($\star$) *Prove that $\vec{\mathbb{S}}^+$ and $\vec{\mathbb{S}}^\omega$ are well-defined.*

Answer to question 2.2

By Question 2.1, $\vec{F}^+ \in \wp(\mathbb{T}^+) \longrightarrow \wp(\mathbb{T}^+)$ is $\subseteq$-monotone so $\mathbf{lfp}^{\subseteq}\, \vec{F}^+$ does exist on the complete lattice $\langle \wp(\mathbb{T}^+), \subseteq, \varnothing, \mathbb{T}^+, \cup, \cap \rangle$ by Tarski's fixpoint theorem [2].

By Question. 2.1, $\vec{F}^\omega \in \wp(\mathbb{T}^\omega) \longrightarrow \wp(\mathbb{T}^\omega)$ is $\subseteq$-monotone so $\mathbf{gfp}^{\subseteq}\, \vec{F}^\omega$ does exist on the complete lattice $\langle \wp(\mathbb{T}^\omega), \subseteq, \varnothing, \mathbb{T}^\omega, \cup, \cap \rangle$ by Tarski's fixpoint theorem [2]. □

Question 2.3 ($\star\star$) *Let L^+ and L^- be a partition of the set L. For all $X, Y \subseteq L$, define $X^+ \triangleq X \cap L^+$, $X^- \triangleq X \cap L^-$, and $(X \sqsubseteq Y) \triangleq (X^+ \subseteq Y^+) \wedge (X^- \supseteq Y^-)$. Let $F \in \wp(L) \longrightarrow \wp(L)$ be $\subseteq$-monotone[2] such that $\forall X \subseteq L : (F(X))^+ = F(X^+)$. Define $F^+(X) \triangleq (F(X^+))^+$, $\mathbb{S}^+ = \boldsymbol{lfp}^{\subseteq}\, F^+$, $F^-(X) \triangleq (\mathbb{S}^+ \cup F(X^-))^-$, $\mathbb{S}^- = \boldsymbol{gfp}^{\subseteq}\, F^-$.*

Prove that $\mathbb{S} \triangleq \mathbb{S}^+ \cup \mathbb{S}^- = \boldsymbol{lfp}^{\sqsubseteq}\, F$.

Answer to question 2.3

$\langle \wp(L), \subseteq \rangle$ is a complete lattice and F is $\subseteq$-monotone when so are F^+ and F^- proving that $\mathbf{lfp}^{\subseteq}\, F^+$ and $\mathbf{gfp}^{\subseteq}\, F^-$ exist by Tarski's fixpoint theorem [2]. We first prove that $\mathbb{S}$ is a fixpoint of F.

$$\begin{array}{lll}
& \mathbb{S} & \\
= & \mathbb{S}^+ \cup \mathbb{S}^- & \\
= & F^+(\mathbb{S}^+) \cup F^-(\mathbb{S}^-) & \\
& & \wr \text{by fixpoint definitions } \mathbb{S}^+ \triangleq \mathbf{lfp}^{\subseteq}\, F^+ \text{ and } \mathbb{S}^- \triangleq \mathbf{gfp}^{\subseteq}\, F^- \int \\
= & (F(\mathbb{S}^+))^+ \cup (F(\mathbb{S}^+ \cup \mathbb{S}^-))^- & \wr \text{def. } F^+ \text{ and } F^- \int \\
= & (F(\mathbb{S}))^+ \cup (F(\mathbb{S}))^- & \wr \text{since } (F(S^+))^+ = (F(S))^+ \text{ and } \mathbb{S} = \mathbb{S}^+ \cup \mathbb{S}^- \int \\
= & F(\mathbb{S}) & \wr \text{since } \forall X \subseteq L : X = X^+ \cup X^- \int
\end{array}$$

[2] but not necessarily $\sqsubseteq$-monotone.

To prove that $\mathbb{S}$ is the $\sqsubseteq$-least fixpoint of F, let T be another fixpoint of F that is $T = F(T)$. It follows that $T^+ \cup T^- = (F(T))^+ \cup (F(T))^-$ so $T^+ = (F(T))^+$ and $T^- = (F(T))^-$ since $L^+ \cap L^- = \varnothing$. Therefore $T^+ = (F(T))^+ = (F(T^+))^+ = F^+(T^+)$ hence $\mathbb{S}^+ \subseteq T^+$ since $\mathbb{S}^+ \triangleq \mathbf{lfp}^{\subseteq} F^+$. Moreover $T^- = (F(T))^- = (F(T^+ \cup T^-))^- \supseteq (F(\mathbb{S}^+ \cup T^-))^- = F^-(T^-)$ by $\subseteq$-monotony of F. It follows that $T^- \subseteq \mathbb{S}^-$ by Tarski's fixpoint theorem [2] for $\mathbf{gfp}^{\subseteq} F^-$. We conclude that $\mathbb{S} \sqsubseteq T$ by def. of $\sqsubseteq$. □

By Question 2.1 and 2.3, it follows that

$$\vec{\mathbb{S}} \triangleq \vec{\mathbb{S}}^+ \cup \vec{\mathbb{S}}^\omega = \mathbf{lfp}^{\sqsubseteq} \vec{F} . \tag{1}$$

Question 2.4 ($\star\star$) *Prove that*

$$\vec{\mathbb{S}} = \mathbf{gfp}^{\subseteq} \vec{F} .$$

Answer to question 2.4

By Question 2.1, $\vec{F}$ is $\subseteq$-monotone so $\mathbf{gfp}^{\subseteq} \vec{F}$ exists by Tarski's fixpoint theorem [2].

By Question 1, $\vec{F}(\mathbf{lfp}^{\sqsubseteq} \vec{F}) = \mathbf{lfp}^{\sqsubseteq} \vec{F}$ so $\mathbf{lfp}^{\sqsubseteq} \vec{F} \subseteq \mathbf{gfp}^{\subseteq} \vec{F}$ by def. $\mathbf{gfp}$, proving $(\mathbf{lfp}^{\sqsubseteq} \vec{F})^+ \subseteq (\mathbf{gfp}^{\subseteq} \vec{F})^+$ and $(\mathbf{lfp}^{\sqsubseteq} \vec{F})^\omega \subseteq (\mathbf{gfp}^{\subseteq} \vec{F})^\omega$. Moreover $\vec{F}(\mathbf{gfp}^{\subseteq} \vec{F}) = \mathbf{gfp}^{\subseteq} \vec{F}$ so $\mathbf{lfp}^{\sqsubseteq} \vec{F} \sqsubseteq \mathbf{gfp}^{\subseteq} \vec{F}$ by def. $\mathbf{lfp}$, proving that $(\mathbf{lfp}^{\sqsubseteq} \vec{F})^\omega \supseteq (\mathbf{gfp}^{\subseteq} \vec{F})^\omega$ hence $(\mathbf{lfp}^{\sqsubseteq} \vec{F})^\omega = (\mathbf{gfp}^{\subseteq} \vec{F})^\omega$ by antisymmetry.

It remains to prove $(\mathbf{lfp}^{\sqsubseteq} \vec{F})^+ \supseteq (\mathbf{gfp}^{\subseteq} \vec{F})^+$. Given a trace $\varsigma \in (\mathbf{gfp}^{\subseteq} \vec{F})^+ = (\vec{F}(\mathbf{gfp}^{\subseteq} \vec{F}))^+$, we prove that $\varsigma \in (\vec{F}(\mathbf{lfp}^{\sqsubseteq} \vec{F}))^+ = (\mathbf{lfp}^{\sqsubseteq} \vec{F})^+$. The case (a) is trivial, the cases (c) and (e) are impossible since ς is finite and cases (b), (d), and (f) follow by induction on the length $|\varsigma|$ of ς. In all these case, we have $\varsigma = f(\sigma, \sigma') \in (\vec{F}(\mathbf{gfp}^{\subseteq} \vec{F}))^+$ with $|\sigma| < |\varsigma|$ and $|\sigma'| < |\varsigma|$ so $\sigma, \sigma' \in (\mathbf{lfp}^{\sqsubseteq} \vec{F})^+$ by induction hypothesis proving that $\varsigma = f(\sigma, \sigma') \in (\vec{F}(\mathbf{lfp}^{\sqsubseteq} \vec{F}))^+ = (\mathbf{lfp}^{\sqsubseteq} \vec{F})^+$ by respective def. (b), (d), and (f) of $\vec{F}$. □

Question 2.5 ($\star\star$) *Prove that the bifinitary trace semantics* $\vec{\mathbb{S}}$ *is* suffix-closed *in that*

$$\forall \sigma \in \mathbb{T}^\infty : \mathsf{a} \bullet \sigma \in \vec{\mathbb{S}} \implies \sigma \in \vec{\mathbb{S}} .$$

Answer to question 2.5

We proceed by structural induction on the closed term a. Assume $\mathsf{a} \bullet \sigma \in \vec{\mathbb{S}} = \vec{F}(\vec{\mathbb{S}})$. The case $\mathsf{a} \bullet \sigma = \mathsf{v}$ is impossible since $\forall \sigma \in \mathbb{T}^\infty : \sigma \neq \epsilon$.

If $\mathsf{a} \bullet \sigma = (\boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{a}')\ \mathsf{v} \bullet \mathsf{a}'[\mathsf{x} \leftarrow \mathsf{v}] \bullet \sigma'$ then $\sigma = \mathsf{a}'[\mathsf{x} \leftarrow \mathsf{v}] \bullet \sigma' \in \vec{\mathbb{S}}$ by def. of $\vec{F}$.

If $\mathsf{a} \bullet \sigma = \sigma'@\mathsf{b}$ where $\sigma' \in \vec{\mathbb{S}}^\omega \subseteq \vec{\mathbb{S}}$ then $\mathsf{a} = (\mathsf{a}'\ \mathsf{b})$ and $\sigma' = \mathsf{a}' \bullet \sigma'' \in \vec{\mathbb{S}}$ so $\sigma'' \in \vec{\mathbb{S}}^\omega \subseteq \vec{\mathbb{S}}$ by induction hypothesis proving that $\sigma = \sigma''@\mathsf{b} \in \vec{F}(\vec{\mathbb{S}}) = \vec{\mathbb{S}}$.

If $\mathsf{a} \bullet \sigma = (\sigma'@\mathsf{b}) \bullet (\mathsf{v}\ \mathsf{b}) \bullet \sigma''$ where $\sigma' \bullet \mathsf{v} \in \vec{\mathbb{S}}^+$ and $(\mathsf{v}\ \mathsf{b}) \bullet \sigma'' \in \vec{\mathbb{S}}$ then $\sigma' = \mathsf{a}' \bullet \sigma'''$ where $\mathsf{a} = (\mathsf{a}'\ \mathsf{b})$ so $\mathsf{a}' \bullet \sigma''' \bullet \mathsf{v} \in \vec{\mathbb{S}}^+ \subseteq \vec{\mathbb{S}}$ proving $\sigma''' \bullet \mathsf{v} \in \vec{\mathbb{S}}^+ \subseteq \vec{\mathbb{S}}$ by induction hypothesis and so $\sigma = (\sigma'''@\mathsf{b}) \bullet (\mathsf{v}\ \mathsf{b}) \bullet \sigma'' \in \vec{F}(\vec{\mathbb{S}}) = \vec{\mathbb{S}}$.

If $\mathsf{a} \bullet \sigma = \mathsf{a}'@\sigma'$ where $\sigma' \in \vec{\mathbb{S}}^\omega \subseteq \vec{\mathbb{S}}$ then $\mathsf{a} = (\mathsf{a}'\ \mathsf{b})$ and $\sigma' = \mathsf{b} \bullet \sigma''$ so $\sigma'' \in \vec{\mathbb{S}}^\omega \subseteq \vec{\mathbb{S}}$ by induction hypothesis proving that $\sigma = \mathsf{a}'@\sigma'' \in \vec{F}(\vec{\mathbb{S}}) = \vec{\mathbb{S}}$.

Finally, if $\mathsf{a} \bullet \sigma = (\mathsf{a}'@\sigma') \bullet (\mathsf{a}'\ \mathsf{v}) \bullet \sigma''$ where $\mathsf{a}', \mathsf{v} \in \mathbb{V}$, $\sigma' \bullet \mathsf{v} \in \vec{\mathbb{S}}^+$, and $(\mathsf{a}'\ \mathsf{v}) \bullet \sigma'' \in \vec{\mathbb{S}}$ then $\mathsf{a} = (\mathsf{a}'\ \mathsf{b})$ and $\sigma' = \mathsf{b} \bullet \sigma'''$ so $\mathsf{b} \bullet \sigma''' \bullet \mathsf{v} \in \vec{\mathbb{S}}^+$ proving that $\sigma''' \bullet \mathsf{v} \in \vec{\mathbb{S}}^+$ by induction hypothesis hence $\sigma = (\mathsf{a}'@\sigma''') \bullet (\mathsf{a}'\ \mathsf{v}) \bullet \sigma'' \in \vec{F}(\vec{\mathbb{S}}) = \vec{\mathbb{S}}$. □

Question 2.6 ($\star$) *Prove that the bifinitary trace semantics $\vec{\mathbb{S}}$ is* total *in that it excludes intermediate or result errors*

$$\forall \mathsf{a} \in \overline{\mathbb{T}} : \nexists \sigma, \sigma' \in \overline{\mathbb{T}}^{\propto}, \mathsf{e} \in \mathbb{E} : \mathsf{a} \bullet \sigma \bullet \mathsf{e} \bullet \sigma' \in \vec{\mathbb{S}} \ .$$

Answer to question 2.6

Assume, by reductio ad absurdum, that $\mathsf{a} \bullet \sigma \bullet \mathsf{e} \bullet \sigma' \in \vec{\mathbb{S}}$ then $\mathsf{e} \bullet \sigma' \in \vec{\mathbb{S}}$ since $\vec{\mathbb{S}}$ is suffix-closed. By structural induction on e, if $\mathsf{e} = \mathsf{e}_1\ \mathsf{a}$ then, by definition of $\vec{\mathbb{S}} = \vec{F}(\vec{\mathbb{S}})$, $\exists \sigma'' : \mathsf{e}_1 \bullet \sigma'' \in \vec{\mathbb{S}}$, which is impossible by induction, or $\mathsf{e} = \mathsf{c}\ \mathsf{a}$ and then $\exists \sigma'' : \mathsf{c} \bullet \sigma'' \in \vec{\mathbb{S}} = \vec{F}(\vec{\mathbb{S}})$ so $\sigma'' = \epsilon$, which excludes all cases (c)–(f), the only possible ones for e. □

Question 2.7 ($\star$) *Prove that the finite maximal traces are* blocking *in that the result of a finite computation is always a final value*

$$\forall \sigma \in \mathbb{T}^{\infty} \cup \{\epsilon\} : \sigma \bullet \mathsf{b} \in \vec{\mathbb{S}}^{+} \implies \mathsf{b} \in \mathbb{V} \ .$$

Answer to question 2.7

By induction on the length of σ and definition of $\vec{\mathbb{S}}^{+} = \vec{F}(\vec{\mathbb{S}}) \cap \mathbb{T}^{+}$. □

3. Relational semantics of the eager λ-calculus

3.1 Relational abstraction of traces

The relational abstraction of sets of traces is

$$\begin{array}{rcl} \alpha & \in & \wp(\mathbb{T}^{\infty}) \longrightarrow \wp(\mathbb{T} \times (\mathbb{T} \cup \{\bot\})) \\ \alpha(S) & \triangleq & \{\langle \sigma_0,\, \sigma_{n-1} \rangle \mid \sigma \in S \wedge |\sigma| = n\} \cup \{\langle \sigma_0,\, \bot \rangle \mid \sigma \in S \wedge |\sigma| = \omega\} \\ \gamma & \in & \wp(\mathbb{T} \times (\mathbb{T} \cup \{\bot\})) \longrightarrow \wp(\mathbb{T}^{\infty}) \\ \gamma(T) & \triangleq & \{\sigma \in \mathbb{T}^{\infty} \mid (|\sigma| = n \wedge \langle \sigma_0,\, \sigma_{n-1} \rangle \in T) \vee (|\sigma| = \omega \wedge \langle \sigma_0,\, \bot \rangle \in T)\} \end{array} \tag{2}$$

Question 3.1 ($\star$) *Prove that*

$$\langle \wp(\mathbb{T}^{\infty}),\, \subseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \wp(\mathbb{T} \times (\mathbb{T} \cup \{\bot\})),\, \subseteq \rangle \ . \tag{3}$$

Answer to question 3.1

$$\begin{array}{ll} & \alpha(S) \subseteq T \\ \iff & \{\langle \sigma_0,\, \sigma_{n-1} \rangle \mid \sigma \in S \wedge |\sigma| = n\} \cup \{\langle \sigma_0,\, \bot \rangle \mid \sigma \in S \wedge |\sigma| = \omega\} \subseteq T \\ & \qquad\qquad \text{⟅def. } \alpha\text{⟆} \\ \iff & \forall \sigma \in S^{+} : \langle \sigma_0,\, \sigma_{|\sigma|-1} \rangle \in T^{+} \wedge \forall \sigma \in S^{\omega} : \langle \sigma_0,\, \bot \rangle \in T^{\omega} \\ & \qquad\qquad \text{⟅def. } \subseteq,\ S^{+} \triangleq S \cap \mathbb{T}^{+}, \text{ and } S^{\omega} \triangleq S \cap \mathbb{T}^{\omega}\text{⟆} \\ \iff & S^{+} \subseteq \{\sigma \mid |\sigma| = n \wedge \langle \sigma_0,\, \sigma_{n-1} \rangle \in T\} \wedge S^{\omega} \subseteq \{\sigma \mid |\sigma| = \omega \wedge \langle \sigma_0,\, \bot \rangle \in T\} \\ & \qquad\qquad \text{⟅def. } \subseteq,\ T^{+} \triangleq T \cap (\mathbb{T} \times \mathbb{T}),\text{ and } T^{\omega} \triangleq T \cap (\sigma\mathbb{T} \times \{\bot\})\text{⟆} \\ \iff & S \subseteq \gamma(T) \qquad\qquad \text{⟅} S = S^{+} \cup S^{\omega} \text{ and def. } \gamma(T)\text{⟆} \end{array}$$

□

The bifinitary relational semantics $\widehat{\mathbb{S}} \triangleq \alpha(\vec{\mathbb{S}}) = \alpha(\mathbf{lfp}^{\sqsubseteq} \vec{F})$ can be defined in fixpoint form as $\mathbf{lfp}^{\sqsubseteq} \widehat{F}$ where the big-step transformer $\widehat{F} \in \wp(\mathbb{T} \times (\mathbb{T} \cup \{\bot\})) \longrightarrow \wp(\mathbb{T} \times (\mathbb{T} \cup \{\bot\}))$ is

$$\begin{array}{rcl} \widehat{F}(T) & \triangleq & \{\langle \mathsf{v},\, \mathsf{v}\rangle \mid \mathsf{v} \in \mathbb{V}\} \cup \\ & & \{\langle (\boldsymbol{\lambda}\, \mathsf{x} \bullet \mathsf{a})\ \mathsf{v},\, r\rangle \mid \mathsf{v} \in \mathbb{V} \wedge \langle \mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}],\, r\rangle \in T\} \cup \\ & & \{\langle (\mathsf{a}\ \mathsf{b}),\, \bot\rangle \mid \langle \mathsf{a},\, \bot\rangle \in T\} \cup \\ & & \{\langle (\mathsf{a}\ \mathsf{b}),\, r\rangle \mid \langle \mathsf{a},\, \mathsf{v}\rangle \in T^+ \wedge \mathsf{v} \in \mathbb{V} \wedge \langle (\mathsf{v}\ \mathsf{b}),\, r\rangle \in T\} \cup \\ & & \{\langle (\mathsf{a}\ \mathsf{b}),\, \bot\rangle \mid \mathsf{a} \in \mathbb{V} \wedge \langle \mathsf{b},\, \bot\rangle \in T\} \cup \\ & & \{\langle (\mathsf{a}\ \mathsf{b}),\, r\rangle \mid \mathsf{a}, \mathsf{v} \in \mathbb{V} \wedge \langle \mathsf{b},\, \mathsf{v}\rangle \in T^+ \wedge \langle (\mathsf{a}\ \mathsf{v}),\, r\rangle \in T\}\ . \end{array} \tag{4}$$

Question 3.2 ($\star$) *Prove that $\widehat{F}$ is $\subseteq$-monotone but not $\sqsubseteq$-monotone.*

Answer to question 3.2

$\subseteq$-monotony holds for the first constant case and $\cup$ and can be proved for all other cases of the form $F(S) = \{f(\mathsf{a}, \mathsf{a}', ..., \sigma, \sigma') \mid p(\mathsf{a}, \mathsf{a}', ...) \wedge g(\sigma) \in S^+ \wedge h(\sigma') \in S\}$ so that $S \subseteq S'$ implies $F(S) \subseteq F(S')$.

The counter-example of Question 2.1, $X = \{\langle(\theta\ \theta),\, \bot\rangle\}$ and $Y = \{\langle \boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{x}\ \theta,\, \theta\rangle, \langle \theta\ \theta,\, \bot\rangle\}$ with $X \sqsubseteq Y$ but $\widehat{F}(X) \not\sqsubseteq \widehat{F}(Y)$ shows the absence of monotony. □

Question 3.3 ($\star\star\star$) *Prove the commutation property $\alpha(\vec{F}(S)) = \widehat{F}(\alpha(S))$*

Answer to question 3.3

α is a complete $\cup$-morphism, so we calculate $\alpha(\vec{F}(S))$ by cases.

— $\alpha(\{\mathsf{v} \in \overline{\mathbb{T}}^{\infty} \mid \mathsf{v} \in \mathbb{V}\})$

$= \{\langle \mathsf{v},\, \mathsf{v}\rangle \mid \mathsf{v} \in \mathbb{V}\}$ ⟅def. α and $|\mathsf{v}| = 1$⟆

— $\alpha(\{(\boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{a})\ \mathsf{v} \bullet \mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}] \bullet \sigma \mid \mathsf{v} \in \mathbb{V} \wedge \mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}] \bullet \sigma \in S\})$

$= \alpha(\{(\boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{a})\ \mathsf{v} \bullet \mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}] \bullet \sigma \mid \mathsf{v} \in \mathbb{V} \wedge \mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}] \bullet \sigma \in S^+\}) \cup$
$\alpha(\{(\boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{a})\ \mathsf{v} \bullet \mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}] \bullet \sigma \mid \mathsf{v} \in \mathbb{V} \wedge \mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}] \bullet \sigma \in S^{\omega}\})$
⟅$S = S^+ \cup S^{\omega}$ and α preserves lubs⟆

$= \{\langle (\boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{a})\ \mathsf{v},\, r\rangle \mid \mathsf{v} \in \mathbb{V} \wedge \langle \mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}],\, r\rangle \in \alpha(S)^+\} \cup$
$\{\langle (\boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{a})\ \mathsf{v},\, \bot\rangle \mid \mathsf{v} \in \mathbb{V} \wedge \langle \mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}],\, \bot\rangle \in \alpha(S)^{\omega}\}$ ⟅def. α⟆

$= \{\langle (\boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{a})\ \mathsf{v},\, r\rangle \mid \mathsf{v} \in \mathbb{V} \wedge \langle \mathsf{a}[\mathsf{x} \leftarrow \mathsf{v}],\, r\rangle \in \alpha(S)\}$
⟅def. $T^+ \triangleq T \cap (\mathbb{T} \times \mathbb{T})$ and $T^{\omega} \triangleq T \cap (\mathbb{T} \times \{\bot\})$⟆

— $\alpha(\{\sigma@\mathsf{b} \mid \sigma \in S^{\omega}\})$

$= \{\langle (\sigma_0\ \mathsf{b}),\, \bot\rangle \mid \sigma \in S^{\omega}\}$ ⟅def. α and @⟆

$= \{\langle (\sigma_0\ \mathsf{b}),\, \bot\rangle \mid \langle \sigma_0,\, \bot\rangle \in \alpha(S)\}$ ⟅def. α⟆

$= \{\langle (\mathsf{a}\ \mathsf{b}),\, \bot\rangle \mid \langle \mathsf{a},\, \bot\rangle \in \alpha(S)\}$ ⟅$S \subseteq \mathbb{T}^{\infty}$ so $\sigma_0 \in \mathbb{T}$⟆

— $\alpha(\{(\sigma@\mathsf{b}) \bullet (\mathsf{v}\ \mathsf{b}) \bullet \sigma' \mid \sigma \bullet \mathsf{v} \in S^+ \wedge \mathsf{v} \in \mathbb{V} \wedge (\mathsf{v}\ \mathsf{b}) \bullet \sigma' \in S\})$

$$
\begin{array}{ll}
= & \alpha(\{(\sigma@\mathsf{b})\bullet(\mathsf{v}\ \mathsf{b})\bullet\sigma' \mid \sigma\bullet\mathsf{v}\in S^+ \wedge \mathsf{v}\in\mathbb{V} \wedge (\mathsf{v}\ \mathsf{b})\bullet\sigma'\in S^+\}) \cup \\
& \alpha(\{(\sigma@\mathsf{b})\bullet(\mathsf{v}\ \mathsf{b})\bullet\sigma' \mid \sigma\bullet\mathsf{v}\in S^+ \wedge \mathsf{v}\in\mathbb{V} \wedge (\mathsf{v}\ \mathsf{b})\bullet\sigma'\in S^\omega\}) \\
& \qquad\qquad \wr S = S^+ \cup S^\omega \text{ and } \alpha \text{ preserves lubs}\int \\
= & \{\langle(\sigma_0\ \mathsf{b}),\ r\rangle \mid \sigma\bullet\mathsf{v}\in S^+ \wedge \mathsf{v}\in\mathbb{V} \wedge \langle(\mathsf{v}\ \mathsf{b}),\ r\rangle\in\alpha(S)^+\} \cup \\
& \{\langle(\sigma\ \mathsf{b}),\ \bot\rangle \mid \sigma\bullet\mathsf{v}\in S^+ \wedge \mathsf{v}\in\mathbb{V} \wedge \langle(\mathsf{v}\ \mathsf{b}),\ \bot\rangle\in\alpha(S)^\omega\}) \qquad \wr \text{def. } \alpha \text{ and } @\int \\
= & \{\langle(\sigma_0\ \mathsf{b}),\ r\rangle \mid \langle\sigma_0,\ \mathsf{v}\rangle\in\alpha(S)^+ \wedge \mathsf{v}\in\mathbb{V} \wedge \langle(\mathsf{v}\ \mathsf{b}),\ r\rangle\in\alpha(S)\} \\
& \qquad\qquad \wr \text{def. } T^+ \triangleq T\cap(\mathbb{T}\times\mathbb{T}),\ T^\omega \triangleq T\cap(\mathbb{T}\times\{\bot\}), \text{ and } \alpha\int \\
= & \{\langle(\mathsf{a}\ \mathsf{b}),\ r\rangle \mid \langle\mathsf{a},\ \mathsf{v}\rangle\in\alpha(S)^+ \wedge \mathsf{v}\in\mathbb{V} \wedge \langle(\mathsf{v}\ \mathsf{b}),\ r\rangle\in\alpha(S)\} \\
& \qquad\qquad \wr S\subseteq\mathbb{T}^\infty \text{ so } \sigma_0\in\mathbb{T}\int
\end{array}
$$

— $\alpha(\{\mathsf{a}@\sigma \mid \mathsf{a}\in\mathbb{V}\wedge\sigma\in S^\omega\})$

$$
\begin{array}{ll}
= & \{\langle(\mathsf{a}\ \sigma_0),\ \bot\rangle \mid \mathsf{a}\in\mathbb{V}\wedge\sigma\in S^\omega\} \qquad \wr \text{def. } \alpha \text{ and } @\int \\
= & \{\langle(\mathsf{a}\ \sigma_0),\ \bot\rangle \mid \mathsf{a}\in\mathbb{V}\wedge\langle\sigma_0,\ \bot\rangle\in\alpha(S)\} \qquad \wr \text{def. } \alpha \text{ and } T^\omega \triangleq T\cap(\mathbb{T}\cup\{\bot\})\int \\
= & \{\langle(\mathsf{a}\ \mathsf{b}),\ \bot\rangle \mid \mathsf{a}\in\mathbb{V}\wedge\langle\mathsf{b},\ \bot\rangle\in\alpha(S)\} \qquad \wr S\subseteq\mathbb{T}^\infty \text{ so } \sigma_0\in\mathbb{T}\int
\end{array}
$$

— $\alpha(\{(\mathsf{a}@\sigma)\bullet(\mathsf{a}\ \mathsf{v})\bullet\sigma' \mid \mathsf{a},\mathsf{v}\in\mathbb{V}\wedge\sigma\bullet\mathsf{v}\in S^+\wedge(\mathsf{a}\ \mathsf{v})\bullet\sigma'\in S\})$

$$
\begin{array}{ll}
= & \alpha(\{(\mathsf{a}@\sigma)\bullet(\mathsf{a}\ \mathsf{v})\bullet\sigma' \mid \mathsf{a},\mathsf{v}\in\mathbb{V}\wedge\sigma\bullet\mathsf{v}\in S^+\wedge(\mathsf{a}\ \mathsf{v})\bullet\sigma'\in S^+\}) \cup \\
& \alpha(\{(\mathsf{a}@\sigma)\bullet(\mathsf{a}\ \mathsf{v})\bullet\sigma' \mid \mathsf{a},\mathsf{v}\in\mathbb{V}\wedge\sigma\bullet\mathsf{v}\in S^+\wedge(\mathsf{a}\ \mathsf{v})\bullet\sigma'\in S^\omega\}) \\
& \qquad\qquad \wr S = S^+\cup S^\omega \text{ and } \alpha \text{ preserves lubs}\int \\
= & \{\langle(\mathsf{a}\ \sigma_0),\ r\rangle \mid \mathsf{a},\mathsf{v}\in\mathbb{V}\wedge\langle\sigma_0,\ \mathsf{v}\rangle\in\alpha(S)^+\wedge\langle(\mathsf{a}\ \mathsf{v}),\ r\rangle\in\alpha(S)^+\} \cup \\
& \{\langle(\mathsf{a}\ \sigma_0),\ \bot\rangle \mid \mathsf{a},\mathsf{v}\in\mathbb{V}\wedge\langle\sigma_0,\ \mathsf{v}\rangle\in\alpha(S)^+\wedge\langle(\mathsf{a}\ \mathsf{v}),\ \bot\rangle\in\alpha(S)^\omega\} \qquad \wr \text{def. } \alpha\int \\
= & \{\langle(\mathsf{a}\ \mathsf{b}),\ r\rangle \mid \mathsf{a},\mathsf{v}\in\mathbb{V}\wedge\langle\mathsf{b},\ \mathsf{v}\rangle\in\alpha(S)\wedge\langle(\mathsf{a}\ \mathsf{v}),\ r\rangle\in\alpha(S)\} \\
& \qquad\qquad \wr T^\omega \triangleq T\cap(\mathbb{T}\cup\{\bot\}) \text{ and } S\subseteq\mathbb{T}^\infty \text{ so } \sigma_0\in\mathbb{T}\int \quad .
\end{array}
$$

Hence, we have the commutation property $\alpha(\vec{F}(S)) = \widehat{F}(\alpha(S))$ when defining $\widehat{F}$ by (4). □

Question 3.4 ($\star$) *Prove that* $\widehat{\mathbb{S}}^+ \triangleq \alpha(\vec{\mathbb{S}}^+) = \mathbf{\mathit{lfp}}^\subseteq \widehat{F}^+$ *where* $\widehat{F}^+(S) \triangleq \widehat{F}(S^+)$.

Answer to question 3.4

To prove that $\alpha(\vec{\mathbb{S}}^+) = \alpha(\mathbf{lfp}^\subseteq \vec{F}^+)$ is equal to $\mathbf{lfp}^\subseteq \widehat{F}^+ = \widehat{\mathbb{S}}^+$, we observe that α preserves $\cup$ and $\alpha\circ\vec{F}^+ = \widehat{F}^+\circ\alpha$ by Question. 3.3 so $\alpha(\mathbf{lfp}^\subseteq \vec{F}^+) = \mathbf{lfp}^\subseteq \widehat{F}^+$ by [1, Th. 3]. □

Question 3.5 ($\star\star\star$) *Prove that* $\widehat{\mathbb{S}}^\omega \triangleq \alpha(\vec{\mathbb{S}}^\omega) = \mathbf{\mathit{gfp}}^\subseteq \widehat{F}^\omega$ *where* $\widehat{F}^\omega(S) \triangleq (\widehat{F}(\widehat{\mathbb{S}}^+\cup S^\omega))^\omega$.

Answer to question 3.5

We must prove that $\alpha(\vec{\mathbb{S}}^\omega) = \alpha(\mathbf{gfp}^\subseteq \vec{F}^\omega)$ is equal to $\mathbf{gfp}^\subseteq \widehat{F}^\omega = \widehat{\mathbb{S}}^\omega$.

— To prove that $\alpha(\mathbf{gfp}^\subseteq \vec{F}^\omega) \subseteq \mathbf{gfp}^\subseteq \widehat{F}^\omega$, we let X^δ, $\delta\in\mathcal{O}$ and $\overline{X}^\delta$, $\delta\in\mathcal{O}$ be the respective transfinite iterates of $\vec{F}^\omega$ and $\widehat{F}^\omega$ from $X^0 = \mathbb{T}^\omega$ and $\overline{X}^0 = \mathbb{T}\times\{\bot\}$ so that $\alpha(X^0)\subseteq\overline{X}^0$ hence $X^0\subseteq\gamma(\overline{X}^0)$ by (3) in Sect. 3.1. Assume, by induction hypothesis, that $\forall\beta<\delta$: $X^\beta\subseteq\gamma(\overline{X}^\beta)$. We have $\forall\beta<\delta$: $(\bigcap_{\beta'<\delta}X^{\beta'})\subseteq\gamma(\overline{X}^\beta)$ hence $(\bigcap_{\beta<\delta}X^\beta)\subseteq(\bigcap_{\beta<\delta}\gamma(\overline{X}^\beta))$ by definition of the greatest lower bound (glb) $\cap$ and theregore $(\bigcap_{\beta<\delta}X^\beta)\subseteq\gamma(\bigcap_{\beta<\delta}\overline{X}^\beta)$ by (3) in Sect. 3.1 so $X^\delta = \vec{F}^\omega(\bigcap_{\beta<\delta}X^\beta)\subseteq\vec{F}^\omega(\gamma(\bigcap_{\beta<\delta}\overline{X}^\beta))$ by monotony. It follows that $X^\delta\subseteq\gamma(\widehat{F}^\omega(\bigcap_{\beta<\delta}\overline{X}^\beta)) = \gamma(\overline{X}^\delta)$ since $\alpha\circ\vec{F}^\omega = \widehat{F}^\omega\circ\alpha$ by Question. 3.3 implies

$\alpha \circ \vec{F}^\omega \circ \gamma = \widehat{F}^\omega \circ \alpha \circ \gamma$ hence $\alpha \circ \vec{F}^\omega \circ \gamma \mathrel{\dot\subseteq} \widehat{F}^\omega$ by (3) in Sect. 3.1 and monotony that is $\vec{F}^\omega \circ \gamma \mathrel{\dot\subseteq} \gamma \circ \widehat{F}^\omega$ by (3) in Sect. 3.1. Hence $\exists \lambda \in \mathcal{O} : \mathbf{gfp}^\subseteq \vec{F}^\omega = X^\lambda \subseteq \gamma(\overline{X}^\lambda) = \gamma(\mathbf{gfp}^\subseteq \widehat{F}^\omega)$ and we conclude by (3) in Sect. refsec:Relational-abstraction-of-traces.

— To prove that $\mathbf{gfp}^\subseteq \widehat{F}^\omega \subseteq \alpha(\mathbf{gfp}^\subseteq \vec{F}^\omega)$, we show that $\forall \langle \mathsf{a},\ \bot\rangle \in \mathbf{gfp}^\subseteq \widehat{F}^\omega : \exists \sigma \in \mathbf{gfp}^\subseteq \vec{F}^\omega : \sigma_0 = \mathsf{a}$. To do so for any $\langle \mathsf{a},\ \bot\rangle \in \mathbf{gfp}^\subseteq \widehat{F}^\omega$, we prove by transfinite induction on δ that

$$\forall \delta \in \mathcal{O} > 0 : \forall \langle \mathsf{a},\ \bot\rangle \in \mathbf{gfp}^\subseteq \widehat{F}^\omega : \exists \sigma \in \mathbb{T}^\omega : \sigma_0 = \mathsf{a} \wedge \sigma \in \bigcap_{\beta<\delta} X^\beta \ .$$

For $\delta = 1$, $\bigcap_{\beta<\delta} X^\beta = X^0 = \mathbb{T}^\omega$ and $\mathsf{a} \in \mathbb{T}$.

Assume by induction hypothesis, that $\exists \sigma \in \mathbb{T}^\omega : \sigma_0 = \mathsf{a} \wedge \forall \eta \in \mathcal{O} : 0 < \eta < \delta : \sigma \in \bigcap_{\beta<\eta} X^\beta$. We have $\sigma \in \bigcap_{\eta<\delta} \bigcap_{\beta<\eta} X^\beta = \bigcap_{\beta<\delta} X^\beta$ et we must show that $\exists \sigma \in \mathbb{T}^\omega : \sigma_0 = \mathsf{a} \wedge \sigma \in X^\delta = \vec{F}^\omega(\bigcap_{\beta<\delta} X^\beta)$. Because the iterates X^δ, $\delta \in \mathcal{O}$ are decreasing, this implies $\exists \sigma \in \mathbb{T}^\omega : \sigma_0 = \mathsf{a} \wedge \sigma \in \bigcap_{\beta<\delta} X^\beta$.

It remains to show, by structural case analysis on a, that if $\sigma \in S : \sigma_0 = \mathsf{a}$, then $\exists \sigma' \in \vec{F}(S) : \sigma'_0 = \mathsf{a}$ where $S = \bigcap_{\beta<\delta} X^\beta$.

— If $\mathsf{a} \in \mathbb{V}$ then $\langle \mathsf{a},\ \bot\rangle \notin \mathbf{gfp}^\subseteq \widehat{F}^\omega$.

— If $\mathsf{a} = (\boldsymbol{\lambda}\, \mathsf{x} \bullet \mathsf{a}')\ \mathsf{v}$, $\mathsf{v} \in \mathbb{V}$ then $\langle \mathsf{a},\ \bot\rangle \in \mathbf{gfp}^\subseteq \widehat{F}^\omega = \widehat{F}^\omega(\mathbf{gfp}^\subseteq \widehat{F}^\omega)$ so by (4), $\langle \mathsf{a}'[\mathsf{x} \leftarrow \mathsf{v}],\ \bot\rangle \in \mathbf{gfp}^\subseteq \widehat{F}^\omega$. By induction on δ, we have $\exists \sigma' \in \mathbb{T}^\omega : \sigma'_0 = \mathsf{a}'[\mathsf{x} \leftarrow \mathsf{v}] \wedge \sigma' \in \bigcap_{\beta<\delta} X^\beta$ so that, by (b), $(\boldsymbol{\lambda}\, \mathsf{x} \bullet \mathsf{a}')\ \mathsf{v} \bullet \mathsf{a}'[\mathsf{x} \leftarrow \mathsf{v}] \bullet \sigma' \in \vec{F}(\bigcap_{\beta<\delta} X^\beta) = X^\delta$.

— If $\mathsf{a} = (\mathsf{a}'\ \mathsf{b})$ then there are four subcases.

— If $\langle \mathsf{a}',\ \bot\rangle \in \mathbf{gfp}^\subseteq \widehat{F}^\omega \subseteq \bigcap_{\beta<\delta} X^\beta$ then, by induction hypothesis on δ, we have $\exists \sigma' \in \mathbb{T}^\omega : \sigma'_0 = \mathsf{a}' \wedge \sigma' \in \bigcap_{\beta<\delta} X^\beta$ so that, by (c), $\sigma'@\mathsf{b} \in \vec{F}(\bigcap_{\beta<\delta} X^\beta) = X^\delta$ is such that $\sigma'_0 = (\mathsf{a}'\ \mathsf{b}) = \mathsf{a}$ by definition of @.

— If $\langle \mathsf{a}',\ \mathsf{v}\rangle \in \widehat{\mathbb{S}}^+ = \alpha(\vec{\mathbb{S}}^+)$, $\mathsf{v} \in \mathbb{V}$, and $\langle (\mathsf{v}\ \mathsf{b}),\ \bot\rangle \in \mathbf{gfp}^\subseteq \widehat{F}^\omega$ then, by induction hypothesis on δ, we have $\exists \sigma' \in \mathbb{T}^\omega : \sigma'_0 = (\mathsf{v}\ \mathsf{b}) \wedge \sigma' \in \bigcap_{\beta<\delta} X^\beta$. By definition (2) of α in Sect. 3.1, there exists $\varsigma \in \mathbb{T}^+ : \varsigma \in \vec{\mathbb{S}}^+ \wedge |\varsigma| = n \wedge \langle \varsigma_0,\ \varsigma_{n-1}\rangle = \langle \mathsf{a}',\ \mathsf{v}\rangle$ proving by definition (d) of $\widehat{F}$ that $\exists \sigma'' = (\varsigma@\mathsf{b}) \fatsemi \sigma' \in \widehat{F}(\bigcap_{\beta<\delta} X^\beta) = X^\delta$ where, by definition, $\varsigma \bullet \mathsf{c} \fatsemi \mathsf{c} \bullet \varsigma' \triangleq \varsigma \bullet \mathsf{c} \bullet \varsigma'$. We have $\sigma''_0 = (\varsigma@\mathsf{b})_0 = (\varsigma_0@\mathsf{b}) = (\mathsf{a}'@\mathsf{b}) = \mathsf{a}$.

— If $\mathsf{a}' \in \mathbb{V}$ and $\langle \mathsf{b},\ \bot\rangle \in \mathbf{gfp}^\subseteq \widehat{F}^\omega$ then by induction hypothesis on δ, $\exists \sigma' \in \mathbb{T}^\omega : \sigma_0 = \mathsf{b} \wedge \sigma' \in \bigcap_{\beta<\delta} X^\beta$ proving by definition (e) of $\widehat{F}$ that $\sigma = \mathsf{a}'@\sigma' \in \widehat{F}(\bigcap_{\beta<\delta} X^\beta) = X^\delta$ with $\sigma_0 = (\mathsf{a}'@\sigma')_0 = (\mathsf{a}'\ \sigma'_0) = (\mathsf{a}'\ \mathsf{b}) = \mathsf{a}$.

— If $\mathsf{a}', \mathsf{v} \in \mathbb{V}$, $\langle \mathsf{b},\ \mathsf{v}\rangle \in \widehat{\mathbb{S}}^+ = \alpha(\vec{\mathbb{S}}^+)$, and $\langle (\mathsf{a}'\ \mathsf{v}),\ \bot\rangle \in \mathbf{gfp}^\subseteq \widehat{F}^\omega$ then, by induction hypothesis on δ, we have $\exists \sigma' \in \mathbb{T}^\omega : \sigma'_0 = (\mathsf{a}'\ \mathsf{v}) \wedge \sigma' \in \bigcap_{\beta<\delta} X^\beta$. By definition (2) in Sect. 3.1 of α, there exists $\varsigma \in \mathbb{T}^+ : \varsigma \in \vec{\mathbb{S}}^+ \wedge |\varsigma| = n \wedge \langle \varsigma_0,\ \varsigma_{n-1}\rangle = \langle \mathsf{b},\ \mathsf{v}\rangle$ proving by definition (f) of $\widehat{F}$ that $(\mathsf{a}'@\varsigma) \fatsemi \sigma' \in \widehat{F}(\bigcap_{\beta<\delta} X^\beta) = X^\delta$ with $\sigma_0 = (\mathsf{a}'@\varsigma)_0 = (\mathsf{a}'\ \varsigma_0) = (\mathsf{a}'\ \mathsf{b}) = \mathsf{a}$. □

Question 3.6 ($\star$) *Prove that* $\widehat{\mathbb{S}} \triangleq \alpha(\vec{\mathbb{S}}) = \alpha(\boldsymbol{lfp}^\sqsubseteq \vec{F}) = \boldsymbol{lfp}^\sqsubseteq \widehat{F}$.

Answer to question 3.6

By (1) and Question 3.3, we have $\vec{\mathbb{S}} = \vec{F}(\vec{\mathbb{S}})$ so $\widehat{\mathbb{S}} \triangleq \alpha(\vec{\mathbb{S}}) = \alpha(\vec{F}(\vec{\mathbb{S}})) = \widehat{F}(\alpha(\vec{\mathbb{S}})) = \widehat{F}(\widehat{\mathbb{S}})$ proving that $\widehat{\mathbb{S}}$ is a fixpoint of $\widehat{F}$. By Questions 3.4, 3.5, and 2.3, we have $\widehat{\mathbb{S}} = \mathbf{lfp}^\sqsubseteq \widehat{F}$. □

Contrary to the case of the trace semantics in Question. 2.4, the relational semantics <u>*cannot*</u> be defined coinductively.

Question 3.7 ($\star\star$) *Prove that* $(\mathit{lfp}^{\sqsubseteq}\,\vec{F})^+ \subsetneq (\mathit{gfp}^{\subseteq}\,\vec{F})^+$ *and* $(\mathit{lfp}^{\sqsubseteq}\,\vec{F})^\omega = (\mathit{gfp}^{\subseteq}\,\vec{F})^\omega$ *so*

$$\vec{\mathbb{S}} \;\neq\; \mathit{gfp}^{\subseteq}\,\vec{F}\ .$$

Answer to question 3.7

By Question 3.2, $\vec{F}$ is $\subseteq$-monotone so $\mathbf{gfp}^{\subseteq}\,\vec{F}$ exists by Tarski's fixpoint theorem [2].

By Question. 3.6, $\vec{F}(\mathbf{lfp}^{\sqsubseteq}\,\vec{F}) = \mathbf{lfp}^{\sqsubseteq}\,\vec{F}$ so $\mathbf{lfp}^{\sqsubseteq}\,\vec{F} \subseteq \mathbf{gfp}^{\subseteq}\,\vec{F}$ by def. $\mathbf{gfp}$, proving $(\mathbf{lfp}^{\sqsubseteq}\,\vec{F})^+ \subseteq (\mathbf{gfp}^{\subseteq}\,\vec{F})^+$ and $(\mathbf{lfp}^{\sqsubseteq}\,\vec{F})^\omega \subseteq (\mathbf{gfp}^{\subseteq}\,\vec{F})^\omega$. Moreover $\vec{F}(\mathbf{gfp}^{\subseteq}\,\vec{F}) = \mathbf{gfp}^{\subseteq}\,\vec{F}$ so $\mathbf{lfp}^{\sqsubseteq}\,\vec{F} \sqsubseteq \mathbf{gfp}^{\subseteq}\,\vec{F}$ by def. $\mathbf{lfp}$, proving that $(\mathbf{lfp}^{\sqsubseteq}\,\vec{F})^\omega \supseteq (\mathbf{gfp}^{\subseteq}\,\vec{F})^\omega$ hence $(\mathbf{lfp}^{\sqsubseteq}\,\vec{F})^\omega = (\mathbf{gfp}^{\subseteq}\,\vec{F})^\omega$ by antisymmetry.

Let $\theta \triangleq \boldsymbol{\lambda}\mathsf{x}\bullet\mathsf{x}\,\mathsf{x}$ and $0 \triangleq \boldsymbol{\lambda}\mathsf{f}\bullet\boldsymbol{\lambda}\mathsf{x}\bullet\mathsf{x}$. $\langle\theta\ \theta,\ 0\rangle$ belongs to $\overline{\mathbb{T}}^\infty$. If $\langle\theta\ \theta,\ 0\rangle = \langle\mathsf{x}\ \mathsf{x}[\mathsf{x} \leftarrow \theta],\ 0\rangle$ belongs to an iterate of $\vec{F}$ then, by def. (4) of $\vec{F}$, $\langle(\boldsymbol{\lambda}\mathsf{x}\bullet\mathsf{x}\,\mathsf{x})\ \theta,\ 0\rangle = \langle\theta\ \theta,\ 0\rangle$ belongs to the next iterate, hence, by transfinite induction on the iterates, to $\mathbf{gfp}^{\subseteq}\,\vec{F}$. However, there is no finite trace in $\vec{\mathbb{S}}$ starting with term $\theta\ \theta$ and ending with term 0 so, by Question. 3.6, $\langle\theta\ \theta,\ 0\rangle \notin \alpha(\vec{\mathbb{S}}) = \mathbf{lfp}^{\sqsubseteq}\,\vec{F}$, proving $(\mathbf{lfp}^{\sqsubseteq}\,\vec{F})^+ \neq (\mathbf{gfp}^{\subseteq}\,\vec{F})^+$. □

References

[1] P. Cousot. Constructive design of a hierarchy of semantics of a transition system by abstract interpretation. *Theoretical Computer Science*, 277(1—2):47–103, 2002.

[2] A. Tarski. A lattice theoretical fixpoint theorem and its applications. *Pacific Journal of Mathematics*, 5:285–310, 1955.