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

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

P. Cousot

Subject 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) $\sqcap$).*

2. Trace semantics of the eager λ-calculus

2.1 Syntax

The syntax of the λ-calculus with constants is

$\mathsf{x}, \mathsf{y}, \mathsf{z}, \ldots$	$\in$	$\mathbb{X}$	variables
c	$\in$	$\mathbb{C}$	constants ($\mathbb{X} \cap \mathbb{C} = \varnothing$)

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

$$
\begin{array}{rcll}
\mathsf{c} & ::= & 0 \mid 1 \mid \ldots & \\
\mathsf{v} & \in & \mathbb{V} & \text{values} \\
\mathsf{v} & ::= & \mathsf{c} \mid \boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{a} & \\
\mathsf{e} & \in & \mathbb{E} & \text{errors} \\
\mathsf{e} & ::= & \mathsf{c}\ \mathsf{a} \mid \mathsf{e}\ \mathsf{a} & \\
\mathsf{a}, \mathsf{a}', \mathsf{a}_1, \ldots, \mathsf{b}, , \ldots & \in & \mathbb{T} & \text{terms} \\
\mathsf{a} & ::= & \mathsf{x} \mid \mathsf{v} \mid \mathsf{a}\ \mathsf{a}' &
\end{array}
$$

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 $\theta \triangleq \boldsymbol{\lambda}\mathsf{x} \bullet \mathsf{x}\ \mathsf{x}$).*

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

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

Define

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

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

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 $F^+(X) \triangleq (F(X^+))^+$, $\mathbb{S}^+ = \mathit{lfp}^{\subseteq} F^+$, $F^-(X) \triangleq (\mathbb{S}^+ \cup F(X^-))^-$, $\mathbb{S}^- = \mathit{gfp}^{\subseteq} F^-$.*

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

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*

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

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

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

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

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

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*

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

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*

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

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

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.*

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

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

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

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

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 $(\boldsymbol{lfp}^{\sqsubseteq}\, \widehat{F})^+ \subsetneq (\boldsymbol{gfp}^{\subseteq}\, \widehat{F})^+$ and $(\boldsymbol{lfp}^{\sqsubseteq}\, \widehat{F})^\omega = (\boldsymbol{gfp}^{\subseteq}\, \widehat{F})^\omega$ so*

$$\widehat{\mathbb{S}} \quad \neq \quad \boldsymbol{gfp}^{\subseteq}\, \widehat{F}\ .$$