Correction of exercices from course 02

MPRI 2–6: Abstract Interpretation,
application to verification and static analysis

Antoine Miné

year 2016–2017

course 02 (correction)
21 September 2016

Question 1: $\mathcal{S}[T]$

(Σ, τ) is a transition system.

The partial finite traces generated by τ are:
$\mathcal{T}[\tau] \stackrel{\text{def}}{=} \{ (\sigma_0, \ldots, \sigma_n) \in \Sigma^+ \mid \forall i < n\colon (\sigma_i, \sigma_{i+1}) \in \tau \}$

The smallest transition system that generates T is:

$$\mathcal{S}[T] \stackrel{\text{def}}{=} \{ (\sigma, \sigma') \in \Sigma^2 \mid \exists (\sigma_0, \ldots, \sigma_n) \in T \wedge i < n\colon \sigma = \sigma_i \wedge \sigma' = \sigma_{i+1} \}$$

($\mathcal{S}[T]$ is the set of transitions appearing within any trace in T)

Question 2: Galois connection

Recall that:

$\mathcal{T}[\tau] \stackrel{\text{def}}{=} \{\, (\sigma_0, \ldots, \sigma_n) \in \Sigma^+ \mid \forall i < n \colon (\sigma_i, \sigma_{i+1}) \in \tau \,\}$

$\mathcal{S}[T] \stackrel{\text{def}}{=} \{\, (\sigma, \sigma') \in \Sigma^2 \mid \exists (\sigma_0, \ldots, \sigma_n) \in T \wedge i < n \colon \sigma = \sigma_i \wedge \sigma' = \sigma_{i+1} \,\}$

We have $(\mathcal{P}(\Sigma^+), \subseteq) \xleftarrow[\mathcal{S}]{\mathcal{T}} \!\!\!\rightarrow (\mathcal{P}(\Sigma \times \Sigma), \subseteq)$.

proof:

$$\begin{aligned}
&\mathcal{S}[T] \subseteq \tau \\
&\iff \forall (\sigma, \sigma') \in \mathcal{S}[T] \colon (\sigma, \sigma') \in \tau \\
&\iff \forall (\sigma, \sigma') \colon (\exists (\sigma_0, \ldots, \sigma_n) \in T \wedge i < n \colon \sigma = \sigma_i \wedge \sigma' = \sigma_{i+1}) \implies (\sigma, \sigma') \in \tau \\
&\iff \forall (\sigma_0, \ldots, \sigma_n) \in T \wedge i < n \colon (\sigma_i, \sigma_{i+1}) \in \tau \\
&\iff \forall (\sigma_0, \ldots, \sigma_n) \in T \colon (\forall i < n \colon (\sigma_i, \sigma_{i+1}) \in \tau) \\
&\iff \forall (\sigma_0, \ldots, \sigma_n) \in T \colon (\sigma_0, \ldots, \sigma_n) \in \mathcal{T}[\tau] \\
&\iff T \subseteq \mathcal{T}[\tau]
\end{aligned}$$

As a consequence $\forall T \colon T \subseteq (\mathcal{T} \circ \mathcal{S})[T]$ and $\forall \tau \colon (\mathcal{S} \circ \mathcal{T})[\tau] \subseteq \tau$.

In fact, we have a Galois embedding: $\forall \tau \colon (\mathcal{S} \circ \mathcal{T})[\tau] = \tau$.

proof: $\mathcal{S}$ is onto as $\forall \tau \colon \mathcal{S}[\tau] = \tau$.

Question 3: Approximation

Recall that:

$\mathcal{T}[\tau] \stackrel{\text{def}}{=} \{ (\sigma_0, \ldots, \sigma_n) \in \Sigma^+ \mid \forall i < n\colon (\sigma_i, \sigma_{i+1}) \in \tau \}$

$\mathcal{S}[T] \stackrel{\text{def}}{=} \{ (\sigma, \sigma') \in \Sigma^2 \mid \exists (\sigma_0, \ldots, \sigma_n) \in T \wedge i < n\colon \sigma = \sigma_i \wedge \sigma' = \sigma_{i+1} \}$

- $T \stackrel{\text{def}}{=} \{a, aa\}$ is not generated by any transition system
- $\mathcal{S}[T] = \{(a, a)\}$
  which generates: $(\mathcal{T} \circ \mathcal{S})[T] \stackrel{\text{def}}{=} a^+ \supsetneq T$

(if a transition appears once in T, it can appear any number of times in $(\mathcal{T} \circ \mathcal{S})[T]$)

Question 4: Exactness conditions

Recall that:

$\mathcal{T}[\tau] \stackrel{\text{def}}{=} \{ (\sigma_0, \ldots, \sigma_n) \in \Sigma^+ \mid \forall i < n \colon (\sigma_i, \sigma_{i+1}) \in \tau \}$

$\mathcal{S}[T] \stackrel{\text{def}}{=} \{ (\sigma, \sigma') \in \Sigma^2 \mid \exists (\sigma_0, \ldots, \sigma_n) \in T \wedge i < n \colon \sigma = \sigma_i \wedge \sigma' = \sigma_{i+1} \}$

Necessary and sufficient conditions for $(\mathcal{T} \circ \mathcal{S})[T] = T$

- Assume that $T = \mathcal{T}[\tau]$ for some τ, then
  - $\forall (\sigma_0, \ldots, \sigma_n) \in T \colon (\sigma_0, \ldots, \sigma_{n-1}) \in T$
  - $\forall (\sigma_0, \ldots, \sigma_n) \in T \colon (\sigma_1, \ldots, \sigma_n) \in T$
  - $\forall (\sigma_0, \ldots, \sigma_n) \in T, (\sigma_n, \ldots, \sigma_m) \in T \colon (\sigma_0, \ldots, \sigma_m) \in T$
  - $\Sigma \subseteq T$

  $\implies$ T is closed by prefix, suffix and junction, and $\Sigma \subseteq T$

- Assume that T is closed by prefix, suffix, junction and $\Sigma \subseteq T$
  - by prefix and suffix: $\forall (\sigma_0, \ldots, \sigma_n) \in T \colon \forall i < n \colon (\sigma_i, \sigma_{i+1}) \in T$
    i.e., $\mathcal{S}[T] \subseteq T$; as $\mathcal{S}[T] \subseteq \Sigma^2$, we get $\mathcal{S}[T] \subseteq T \cap \Sigma^2$
  - by junction: $\forall i < n \colon (\sigma_i, \sigma_{i+1}) \in T \implies (\sigma_0, \ldots, \sigma_n) \in T$
    together with $\Sigma \subseteq T$, we get $\mathcal{T}[T \cap \Sigma^2] \subseteq T$

  $\implies (\mathcal{T} \circ \mathcal{S})[T] \subseteq T$, hence $(\mathcal{T} \circ \mathcal{S})[T] = T$

Question 5: Galois connection

$$\mathcal{T}_\infty[\tau] \stackrel{\text{def}}{=} \mathcal{T}[\tau] \cup \{\, (\sigma_0, \ldots) \in \Sigma^\omega \mid \forall i \colon (\sigma_i, \sigma_{i+1}) \in \tau \,\}$$

$$\begin{aligned}\mathcal{S}_\infty[T] \stackrel{\text{def}}{=} \{\, (\sigma, \sigma') \in \Sigma^2 \mid\ & \exists (\sigma_0, \ldots, \sigma_n) \in T \cap \Sigma^+ \colon \exists i < n \colon \sigma = \sigma_i \wedge \sigma' = \sigma_{i+1} \vee \\ & \exists (\sigma_0, \ldots) \in T \cap \Sigma^\omega \colon \exists i \colon \sigma = \sigma_i \wedge \sigma' = \sigma_{i+1} \,\}\end{aligned}$$

We have $(\mathcal{P}(\Sigma^\infty), \subseteq) \underset{\mathcal{S}_\infty}{\overset{\mathcal{T}_\infty}{\leftrightarrows}} (\mathcal{P}(\Sigma \times \Sigma), \subseteq)$.

proof: very similar to question 2

$$\begin{aligned}
& \mathcal{S}_\infty[T] \subseteq \tau \\
\iff\ & \forall (\sigma, \sigma') \in \mathcal{S}_\infty[T] \colon (\sigma, \sigma') \in \tau \\
\iff\ & \forall (\sigma_0, \ldots, \sigma_n) \in T \cap \Sigma^+ \colon \forall i < n \colon (\sigma_i, \sigma_{i+1}) \in \tau \\
& \wedge \forall (\sigma_0, \ldots) \in T \cap \Sigma^\omega \colon \forall i \colon (\sigma_i, \sigma_{i+1}) \in \tau \\
\iff\ & \forall (\sigma_0, \ldots, \sigma_n) \in T \cap \Sigma^+ \colon (\sigma_0, \ldots, \sigma_n) \in \mathcal{T}[\tau] \\
& \wedge \forall (\sigma_0, \ldots) \in T \cap \Sigma^\omega \colon (\sigma_0, \ldots) \in \mathcal{T}[\tau] \\
\iff\ & T \cap \Sigma^+ \subseteq \mathcal{T}[\tau] \wedge T \cap \Sigma^\omega \subseteq \mathcal{T}[\tau] \\
\iff\ & T \subseteq \mathcal{T}[\tau]
\end{aligned}$$

We also have a Galois embedding.

Question 6: Approximation

Recall that:
$\mathcal{T}_\infty[\tau] \stackrel{\text{def}}{=} \mathcal{T}[\tau] \cup \{\, (\sigma_0, \ldots) \in \Sigma^\omega \mid \forall i \colon (\sigma_i, \sigma_{i+1}) \in \tau \,\}$
$\mathcal{S}_\infty[T] \stackrel{\text{def}}{=} \{\, (\sigma, \sigma') \in \Sigma^2 \mid$
$\exists (\sigma_0, \ldots, \sigma_n) \in T \cap \Sigma^+ \colon \exists i < n \colon \sigma = \sigma_i \wedge \sigma' = \sigma_{i+1} \vee$
$\exists (\sigma_0, \ldots) \in T \cap \Sigma^\omega \colon \exists i \colon \sigma = \sigma_i \wedge \sigma' = \sigma_{i+1} \,\}$

Consider $T \stackrel{\text{def}}{=} a^+$ (with $\Sigma \stackrel{\text{def}}{=} \{a\}$).

T is closed by prefix, suffix and junction, and $\Sigma \subseteq T$.

We have $\mathcal{S}_\infty[T] = \{(a, a)\}$.

But then, $(\mathcal{T}_\infty \circ \mathcal{S}_\infty)[T] = a^\infty \supsetneq a^+ = T$.

($\mathcal{T}_\infty \circ \mathcal{S}_\infty$ adds infinite traces to sets of finite traces)

Question 7: Exactness conditions

Necessary and sufficient conditions for $(\mathcal{T}_\infty \circ \mathcal{S}_\infty)[T] = T$

- T must be closed by prefix, suffix, junction and contain Σ
- and T must be closed by limit:
  given $(\sigma_0, \ldots) \in \Sigma^\omega$, $\forall n$: $(\sigma_0, \ldots, \sigma_n) \in T \implies (\sigma_0, \ldots) \in T$

proof:
$\forall \tau$: $\mathcal{T}_\infty[\tau]$ is closed by limit, so, it is a necessary condition.

Assume now that T is closed by prefix, suffix, junction and contain Σ, then, by question 4: $(\mathcal{T}_\infty \circ \mathcal{S}_\infty)[T] \cap \Sigma^+ = T \cap \Sigma^+$.

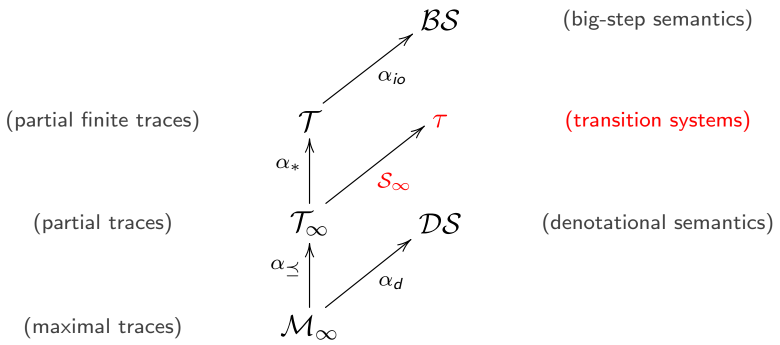
We denote by $\lim : \mathcal{P}(\Sigma^\infty) \to \mathcal{P}(\Sigma^\infty)$ the closure by limit.

Note that $(\mathcal{T}_\infty \circ \mathcal{S}_\infty)[T] = \lim((\mathcal{T}_\infty \circ \mathcal{S}_\infty)[T] \cap \Sigma^+)$.
By hypothesis, $\lim(T) = T$; by monotonicity of lim, $\lim(T \cap \Sigma^+) \subseteq \lim(T)$, hence $\lim(T \cap \Sigma^+) \subseteq T$.

In general, the equality does not hold (T may have infinite traces that are not limits of finite ones); however, as T is closed by prefix, $T \cap \Sigma^+$ contains all finite prefixes of traces in $T \cap \Sigma^\omega$, hence $\lim(T \cap \Sigma^+) = T$.

Hence, $(\mathcal{T}_\infty \circ \mathcal{S}_\infty)[T] = T$.

Note: Hierarchy of semantics



Transition systems are (relational) abstractions of traces semantics.