Correction of exercises from course 02

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

Antoine Miné

Year 2018–2019

Course 02 (correction)
18 September 2018
Question 1: $S[T]$

$(\Sigma, \tau)$ is a transition system.

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

The smallest transition system that generates $T$ is:
$$S[T] \overset{\text{def}}{=} \{ (\sigma, \sigma') \in \Sigma^2 | \exists (\sigma_0, \ldots, \sigma_n) \in T \land i < n: \sigma = \sigma_i \land \sigma' = \sigma_{i+1} \}$$

($S[T]$ is the set of transitions appearing within any trace in $T$)
Question 2: Galois connection

Recall that:
\[ T[\tau] \overset{\text{def}}{=} \{ (\sigma_0, \ldots, \sigma_n) \in \Sigma^+ \mid \forall i < n: (\sigma_i, \sigma_{i+1}) \in \tau \} \]
\[ S[T] \overset{\text{def}}{=} \{ (\sigma, \sigma') \in \Sigma^2 \mid \exists (\sigma_0, \ldots, \sigma_n) \in T \land i < n: \sigma = \sigma_i \land \sigma' = \sigma_{i+1} \} \]

We have \((\mathcal{P}(\Sigma^+), \subseteq) \xrightarrow{T} (\mathcal{P}(\Sigma \times \Sigma), \subseteq)\).

Proof:
\[ S[T] \subseteq \tau \iff \forall (\sigma, \sigma') \in S[T]: (\sigma, \sigma') \in \tau \]
\[ \iff \forall (\sigma, \sigma'): (\exists (\sigma_0, \ldots, \sigma_n) \in T \land i < n: \sigma = \sigma_i \land \sigma' = \sigma_{i+1} \) \implies (\sigma, \sigma') \in \tau \]
\[ \iff \exists (\sigma_0, \ldots, \sigma_n) \in T \land i < n: (\sigma_i, \sigma_{i+1}) \in \tau \]
\[ \iff \forall (\sigma_0, \ldots, \sigma_n) \in T: (\forall i < n: (\sigma_i, \sigma_{i+1}) \in \tau) \]
\[ \iff \forall (\sigma_0, \ldots, \sigma_n) \in T: (\sigma_0, \ldots, \sigma_n) \in T[\tau] \]
\[ \iff T \subseteq T[\tau] \]

As a consequence \(\forall T: T \subseteq (T \circ S)[T]\) and \(\forall \tau: (S \circ T)[\tau] \subseteq \tau\).

In fact, we have a **Galois embedding**: \(\forall \tau: (S \circ T)[\tau] = \tau\).

Proof: \(S\) is onto as \(\forall \tau: S[\tau] = \tau\).
Question 3: Approximation

Recall that:
\[ T[\tau] \overset{\text{def}}{=} \{ (\sigma_0, \ldots, \sigma_n) \in \Sigma^+ | \forall i < n: (\sigma_i, \sigma_{i+1}) \in \tau \} \]
\[ S[T] \overset{\text{def}}{=} \{ (\sigma, \sigma') \in \Sigma^2 | \exists (\sigma_0, \ldots, \sigma_n) \in T \land i < n: \sigma = \sigma_i \land \sigma' = \sigma_{i+1} \} \]

- \( T \overset{\text{def}}{=} \{ a, aa \} \) is not generated by any transition system
- \( S[T] = \{(a, a)\} \)

which generates: \( (T \circ S)[T] \overset{\text{def}}{=} a^+ \supseteq T \)

(if a transition appears once in \( T \), it can appear any number of times in \( (T \circ S)[T] \))
Question 4: Exactness conditions

Recall that:

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

\[ S[T] \overset{\text{def}}{=} \{ (\sigma, \sigma') \in \Sigma^2 \mid \exists (\sigma_0, \ldots, \sigma_n) \in T \land i < n: \sigma = \sigma_i \land \sigma' = \sigma_{i+1} \} \]

**Necessary and sufficient conditions for \((T \circ S)[T] = T\)**

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

  \[ \implies T \text{ is closed by prefix, suffix and junction, and } \Sigma \subseteq T \]

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

  \[ \implies (T \circ S)[T] \subseteq T, \text{ hence } (T \circ S)[T] = T \]
Question 5: Galois connection

\[ T_\infty[\tau] \overset{\text{def}}{=} T[\tau] \cup \{ (\sigma_0, \ldots) \in \Sigma^\omega \mid \forall i: (\sigma_i, \sigma_{i+1}) \in \tau \} \]

\[ S_\infty[T] \overset{\text{def}}{=} \{ (\sigma, \sigma') \in \Sigma^2 \mid \exists (\sigma_0, \ldots, \sigma_n) \in T \cap \Sigma^+ : \exists i < n: \sigma = \sigma_i \land \sigma' = \sigma_{i+1} \lor \exists (\sigma_0, \ldots) \in T \cap \Sigma^\omega : \exists i: \sigma = \sigma_i \land \sigma' = \sigma_{i+1} \} \]

We have \((\mathcal{P}(\Sigma^\infty), \subseteq) \xleftrightarrow{S_\infty} (\mathcal{P}(\Sigma^+ \times \Sigma^\omega), \subseteq)\).

proof: very similar to question 2

\[ S_\infty[T] \subseteq \tau \]
\[ \iff \forall (\sigma, \sigma') \in S_\infty[T]: (\sigma, \sigma') \in \tau \]
\[ \iff \forall (\sigma_0, \ldots, \sigma_n) \in T \cap \Sigma^+: \forall i < n: (\sigma_i, \sigma_{i+1}) \in \tau \land \forall (\sigma_0, \ldots) \in T \cap \Sigma^\omega : \forall i: (\sigma_i, \sigma_{i+1}) \in \tau \]
\[ \iff \forall (\sigma_0, \ldots, \sigma_n) \in T \cap \Sigma^+: (\sigma_0, \ldots, \sigma_n) \in T[\tau] \land \forall (\sigma_0, \ldots) \in T \cap \Sigma^\omega : (\sigma_0, \ldots) \in T[\tau] \]
\[ \iff T \cap \Sigma^+ \subseteq T[\tau] \land T \cap \Sigma^\omega \subseteq T[\tau] \]
\[ \iff T \subseteq T[\tau] \]

We also have a Galois embedding.
Question 6: Approximation

Recall that:
\[
T_\infty[\tau] \overset{\text{def}}{=} T[\tau] \cup \{(\sigma_0, \ldots) \in \Sigma^\omega \mid \forall i: (\sigma_i, \sigma_{i+1}) \in \tau\}
\]

\[
S_\infty[T] \overset{\text{def}}{=} \{(\sigma, \sigma') \in \Sigma^2 \mid \exists (\sigma_0, \ldots, \sigma_n) \in T \cap \Sigma^+: \exists i < n: \sigma = \sigma_i \land \sigma' = \sigma_{i+1} \lor \exists (\sigma_0, \ldots) \in T \cap \Sigma^\omega: \exists i: \sigma = \sigma_i \land \sigma' = \sigma_{i+1}\}
\]

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

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

We have \( S_\infty[T] = \{(a, a)\} \).

But then, \( (T_\infty \circ S_\infty)[T] = a^\infty \supseteq a^+ = T \).

(\( T_\infty \circ S_\infty \) adds infinite traces to sets of finite traces)
Question 7: Exactness conditions

Necessary and sufficient conditions for \((T_\infty \circ S_\infty)[T] = T\)

- \(T\) must be closed by prefix, suffix, junction and contain \(\Sigma\)
- 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:

\(\forall \tau: T_\infty[\tau]\) is closed by limit, so, it is a necessary condition.

Assume now that \(T\) is closed by prefix, suffix, junction and contain \(\Sigma\), then, by question 4: \((T_\infty \circ S_\infty)[T] \cap \Sigma^+ = T \cap \Sigma^+\).

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

Note that \((T_\infty \circ S_\infty)[T] = \text{lim}((T_\infty \circ S_\infty)[T] \cap \Sigma^+)\).

By hypothesis, \(\text{lim}(T) = T\); by monotonicity of \(\text{lim}\), \(\text{lim}(T \cap \Sigma^+) \subseteq \text{lim}(T)\), hence \(\text{lim}(T \cap \Sigma^+) \subseteq T\).

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 \(\text{lim}(T \cap \Sigma^+) = T\).

Hence, \((T_\infty \circ S_\infty)[T] = T\).
Transition systems are (relational) abstractions of traces semantics.