Theoretical Foundations of the UML

Lecture 11: Safe Realisability

Joost-Pieter Katoen

Lehrstuhl für Informatik 2
Software Modeling and Verification Group

moves.rwth-aachen.de/teaching/ss-20/fuml/

May 25, 2020
Outline

1. Safe realisability

2. Closure and inference revisited

3. Characterisation and complexity of safe realisability
Overview

1. Safe realisability

2. Closure and inference revisited

3. Characterisation and complexity of safe realisability
From requirements to implementation

Realisability problem

**Input:** a set of MSCs

**Output:** a CFM $A$ such that $\mathcal{L}(A)$ equals the set of input MSCs.

Questions:

1. Is this possible? (That is, is this decidable?)
2. If so, how complex is it to obtain such CFM?
3. If so, how do such algorithms work?
## Problem variants (1)

### Realisability problem

**Input:** a set of MSCs

**Output:** a CFM $A$ such that $\mathcal{L}(A)$ equals the set of input MSCs.

### Different forms of requirements

- Consider finite sets of MSCs, given as an enumerated set: \{M_1,...,M_k\}
- Consider MSGs, that may describe an infinite set of MSCs.
- Consider MSCs whose set of linearisations is a regular word language.
- Consider MSGs that are non-local choice.
Problem variants (2)

Realisability problem

**Input**: a set of MSCs

**Output**: a CFM $A$ such that $\mathcal{L}(A)$ equals the set of input MSCs.

Different system models

- Consider CFMs without synchronisation messages.
- Allow CFMs that may deadlock. Possibly, a realisation deadlocks.
- Forbid CFMs that deadlock. No realisation will ever deadlock.
- Consider CFMs that are deterministic.
- Consider CFMs that are bounded.
- ......

outputs

✓

tf

- bounded

I

- bounded
Today’s lecture

Today’s setting

Realisation of a finite set of MSCs by a deadlock-free weak CFM.

Results:

1. Conditions for realisability of a finite set of MSCs by a deadlock-free weak CFM.
2. Checking safe realisability by deadlock-free CFMs is in P. (Realisability for weak CFMs that may deadlock is co-NP complete.)

Joost-Pieter Katoen
Theoretical Foundations of the UML
Today’s lecture

Today’s setting

Realisation of a finite set of MSCs by a deadlock-free weak CFM.

Realisation of a finite set of well-formed words (＝ language) by a deadlock-free weak CFM.

This is known as safe realisability.

Results:

1. Conditions for realisability of a finite set of MSCs by a deadlock-free weak CFM.
2. Checking safe realisability by deadlock-free CFMs is in P. (Realisability for weak CFMs that may deadlock is co-NP complete.)
Realisation of a finite set of MSCs by a deadlock-free weak CFM.

Realisation of a finite set of well-formed words (= language) by a deadlock-free weak CFM.

This is known as safe realisability.
Today's lecture

Today's setting

Realisation of a finite set of MSCs by a deadlock-free weak CFM.
Realisation of a finite set of well-formed words (= language) by a deadlock-free weak CFM.
This is known as safe realisability.

This is the setting of the previous lecture, but now focusing on deadlock-free CFMs

Results:

1. Conditions for realisability of a finite set of MSCs by a deadlock-free weak CFM.
Today’s lecture

Today’s setting
Realisation of a finite set of MSCs by a **deadlock-free weak** CFM.
Realisation of a finite set of well-formed words (= language) by a **deadlock-free weak** CFM.
This is known as **safe realisability**.

This is the setting of the previous lecture, but now focusing on deadlock-free CFMs.

Results:
1. Conditions for realisability of a finite set of MSCs by a **deadlock-free weak** CFM.
2. Checking **safe realisability** by deadlock-free CFMs is in **P**.
Today’s lecture

Today’s setting

Realisation of a finite set of MSCs by a deadlock-free weak CFM.

Realisation of a finite set of well-formed words (= language) by a deadlock-free weak CFM.

This is known as safe realisability.

This is the setting of the previous lecture, but now focusing on deadlock-free CFMs.

Results:

1. Conditions for realisability of a finite set of MSCs by a deadlock-free weak CFM.
2. Checking safe realisability by deadlock-free CFMs is in P. (Realisability for weak CFMs that may deadlock is co-NP complete.)
Safe realisability

Possibly a set of MSCs is realisable only by a CFM that may deadlock

Realisation of \( \{ M_1, M_2 \} \) by a weak CFM:

Deadlock occurs when, e.g., \( p \) sends \( a \) and \( q \) sends \( b \)
Safe realisability

Definition (Safe realisability)

1. MSC $M$ is **safely realisable** whenever $\{M\} = \mathcal{L}(\mathcal{A})$ for some 
deadlock-free CFM $\mathcal{A}$.

2. A finite set $\{M_1, \ldots, M_n\}$ of MSCs is **safely realisable** whenever 
$\{M_1, \ldots, M_n\} = \mathcal{L}(\mathcal{A})$ for some **deadlock-free** CFM $\mathcal{A}$.

3. MSG $G$ is **safely realisable** whenever $\mathcal{L}(G) = \mathcal{L}(\mathcal{A})$ for some 
deadlock-free CFM $\mathcal{A}$.

Phrased using linearisations

$L \subseteq Act^*$ is **safely realisable** if $L = Lin(\mathcal{A})$ for some **deadlock-free** CFM $\mathcal{A}$.

Note:

Safe realisability implies realisability, but the converse does not hold.
Overview

1. Safe realisability

2. Closure and inference revisited

3. Characterisation and complexity of safe realisability
Definition (Inference relation and closure)

For well-formed \( L \subseteq Act^* \), and well-formed word \( w \in Act^* \), let:

\[
L \models w \quad \text{iff} \quad (\forall p \in \mathcal{P}. \exists v \in L. w \mid p = v \mid p)
\]

Language \( L \) is \textbf{closed} under \( \models \) whenever for every well-formed \( w \in Act^* \), it holds:

\( L \models w \) implies \( w \in L \).

\[P_1 : \ \omega \neg p_1 = \nu \neg p_1 \quad \text{\&}\quad P_2 : \ \omega \neg p_2 = \nu \neg p_2\]
Weak closure

Definition (Inference relation and closure)
For well-formed \( L \subseteq \text{Act}^* \), and well-formed word \( w \in \text{Act}^* \), let:

\[
L \models w \iff ( \forall p \in \mathcal{P}. \exists v \in L. w \upharpoonright p = v \upharpoonright p)
\]

Language \( L \) is closed under \( \models \) whenever for every \( w \in \text{Act}^* \), it holds: \( L \models w \) implies \( w \in L \).

Definition (Weak closure)
Language \( L \) is weakly closed under \( \models \) whenever for every well-formed prefix \( w \) of some word in \( L \), it holds \( L \models w \) implies \( w \in L \).

Weak closure thus restricts "closure under \( \models \)" to well-formed prefixes in \( L \) only. So far, closure was required for all \( w \in \text{Act}^* \).
Deadlock-free closure

For language $L$, let $\text{pref}(L) = \{w \mid \exists u. w \cdot u \in L\}$ the set of prefixes of $L$.

**Definition ((Deadlock-free) Inference relation)**

For well-formed $L \subseteq \text{Act}^*$, and proper word $w \in \text{Act}^*$, i.e., $w$ is a prefix of a well-formed word, let:

$$L \models \text{df} w \iff (\forall p \in P. \exists v \in \text{pref}(L). w \upharpoonright p \text{ is a prefix of } v \upharpoonright p)$$

**Intuition**
The closure condition asserts that the set of partial MSCs (i.e., prefixes of $L$) can be constructed from the projections of the MSCs in $L$ onto individual processes.
Deadlock-free closure

For language $L$, let $\text{pref}(L) = \{w \mid \exists u. w \cdot u \in L\}$ the set of prefixes of $L$.

**Definition ((Deadlock-free) Inference relation)**

For well-formed $L \subseteq \text{Act}^*$, and proper word $w \in \text{Act}^*$, i.e., $w$ is a prefix of a well-formed word, let:

$$L \models^{df} w \iff (\forall p \in \mathcal{P}. \exists v \in \text{pref}(L). w \upharpoonright p \text{ is a prefix of } v \upharpoonright p)$$

**Definition (Closure under $\models^{df}$)**

Language $L$ is **closed** under $\models^{df}$ whenever $L \models^{df} w$ implies $w \in \text{pref}(L)$.

Intuition

The closure condition asserts that the set of partial MSCs (i.e., prefixes of $L$) can be constructed from the projections of the MSCs in $L$ onto individual processes.
Partial MSC
Deadlock-free closure

For language $L$, let $\text{pref}(L) = \{w \mid \exists u. w \cdot u \in L\}$ the set of prefixes of $L$.

**Definition ((Deadlock-free) Inference relation)**

For well-formed $L \subseteq \text{Act}^*$, and proper word $w \in \text{Act}^*$, i.e., $w$ is a prefix of a well-formed word, let:

$$L \models df w \iff (\forall p \in \mathcal{P}. \exists v \in \text{pref}(L). w \upharpoonright p \text{ is a prefix of } v \upharpoonright p)$$

**Definition (Closure under $\models df$)**

Language $L$ is closed under $\models df$ whenever $L \models df w$ implies $w \in \text{pref}(L)$.

**Intuition**

The closure condition asserts that the set of partial MSCs (i.e., prefixes of $L$) can be constructed from the projections of the MSCs in $L$ onto individual processes.
Example

$L = Lin(\{M_1, M_2\})$ is not closed under $\models^{df}$:

$$w = !(p,q,a)!(q,p,b) \notin \text{pref}(L)$$

But: $L \models^{df} w$ since $w$ is a proper prefix of a well-formed word, and

- for process $p$, there exists $u \in L$ with $w \mid p = !(p,q,a) \in \text{pref}(\{u \mid p\})$, and
- for process $q$, there exists $v \in L$ with $w \mid q = !(q,p,b) \in \text{pref}(\{v \mid q\})$.

Note that $L$ is closed under $\models$. So this shows that closure under $\models^{df}$ does not imply closure under $\models^{df}$.
Deadlock-free weak CFM are closed under $\models^{df}$

**Lemma:**
For every deadlock-free weak CFM $A$, $Lin(A)$ is closed under $\models^{df}$.

**Proof.**
Similar proof strategy as for the closure of weak CFMs under $\models$ (see previous lecture).
Deadlock-free weak CFM are closed under $|=^{df}$

**Lemma:**
For every **deadlock-free** weak CFM $A$, $Lin(A)$ is closed under $|=^{df}$.

**Proof.**
Similar proof strategy as for the closure of weak CFMs under $|=^{df}$ (see previous lecture). Basic intuition is that if $w|p$ is a prefix of $v^p|p$, then from the point of view of process $p$, $w$ can be prolonged with a word $u$, say, such that $w \cdot u = v^p$. This applies to all processes, and as the weak CFM is deadlock-free, such continuation is always possible.  

Joost-Pieter Katoen
Theoretical Foundations of the UML
Overview

1. Safe realisability
2. Closure and inference revisited
3. Characterisation and complexity of safe realisability
Characterisation of safe realisability

Theorem: \[ \text{[Alur et al., 2001]} \]

\( L \subseteq Act^* \) is \textbf{safely realisable} iff \( L \) is \textbf{weakly closed under} \( \models \) and closed under \( \models^d \).

\textbf{1}\hspace{1cm} \text{necessary condition}

\textbf{2}\hspace{1cm} \text{closure under } \models \text{ for all well-formed prefixes of } L

\textbf{2}\hspace{1cm} \text{sufficient + necessary condition}
Theorem: [Alur et al., 2001]

$L \subseteq Act^*$ is **safely** realisable iff $L$ is **weakly** closed under $|=$ and closed under $|=^{df}$.

Proof

On the black board.
Theorem: $L$ is safely realisable if and only if

1. $L$ is weakly closed under $\models$, and
2. $L$ is closed under $\models_{df}$.

Proof: "$\Rightarrow"$. Assume $L$ is safely realisable. Then

a. $L$ is realisable, and by the theorem of lecture 9, it follows $L$ is closed under $\models$.

This implies $L$ is weakly closed under $\models$.

b. There is some deadlock-free (CFM $A$) s.t. $Lin(A) = L$. As $A$ is deadlock-free and weak, it follows by the lemma in this lecture that $Lin(A) = L$ is closed under $\models_{df}$. 
"⇐": Assume $L$ is weakly closed under $F$, and $L$ is closed under $F^{df}$. Let $L_p = \{ \omega \mid \omega \in L \}$, for any process $p$. Since $L$ is finite, $L_p$ is a regular word language. Let $A_p$ be a DFA with state set $Q_p$, initial state $s_{init}$ and accept states $F_p$, with $L(A_p) = L_p$.

W.l.o.g. assume that all states in $A_p$ are productive, i.e., for any state $q \in Q_p$ it is possible to reach some state in $F_p$.

Now let $CFM_A = \left( (A_p)_{p \in P}, s_{init}, F \right)$ with

$S_{init} = \bigcup_{p \in P} s_{init}^p$ and $F = \bigcup_{p \in P} F_p$.

Claim: 1. $Lin(A) = L$ and 2. $CFM_A$ is deadlock-free.

(Obviously, then $L$ is safe realizable).

Proof:

① "⇐": let $w \in L$. Then for every $p$, $w \in L_p$. Thus DFA $A_p$ has an accepting run on $w$, and as $F = \bigcup_{p \in P} F_p$, $CFM_A$ has an accepting run on $w$. 
⊆: let \( w \in \text{Lin}(A) \). As \( \text{Lin}(A) \) is well-formed, \( w \) is well-formed. Since \( F = \bigwedge_{p} F_p \), it follows \( wF_p \in L_p \) for each process \( p \). Thus \( L = w \). Since \( L \) is weakly closed under \( \preceq \), and \( w \) is well-formed, it follows \( w \in L \).

2. \( A \) is deadlock free. This is proven as follows. Assume \( A \) has read the input word \( w \in \text{Act}^* \). \( w \) may be either accepted or not. If it is accepted, there is nothing to prove. Assume \( w \) is not accepted. As CFM \( A \) has successfully read \( w \), it follows \( wF_p \) is a prefix of a word in \( L_p \), for every process \( p \). Since \( L \) is closed under \( \preceq \), it follows that \( w \in \text{pref}(L) \). Let \( w.u \in L \) for \( u \in \Sigma \). As \( F_p \) is deterministic, it has a unique (local) accepting run for \( (w.u)F_p \). This applies to every process \( p \). As \( F = \bigwedge_{p} F_p \), it follows that CFM \( A \) has a unique accepting run for \( w.u.u \). As this applies to every \( w \), it follows that \( A \) is deadlock-free.
Theorem: [Alur et al., 2001]

\[ L \subseteq \text{Act}^* \text{ is safely realisable iff } L \text{ is weakly closed under } \models \text{ and closed under } \models^{df}. \]

Proof

On the black board.

Corollary

The finite set of MSCs \( \{M_1, \ldots, M_n\} \) is safely realisable iff \( \bigcup_{i=1}^{n} Lin(M_i) \) is closed under \( \models \) and \( \models^{df} \).
Theorem

For any well-formed $L \subseteq \text{Act}^*$:

$L$ is regular and closed under $|=\$ if and only if

$L = Lin(\mathcal{A})$ for some $\forall$-bounded weak CFM $\mathcal{A}$.

Theorem

For any well-formed $L \subseteq \text{Act}^*$:

$L$ is regular, weakly closed under $|=\$ and closed under $|=^{df}$ if and only if

$L = Lin(\mathcal{A})$ for some $\forall$-bounded deadlock-free weak CFM $\mathcal{A}$. 
The decision problem “is a given set of MSCs safely realisable?” is in P.

1. set of MSCs is weakly closed under \( \vdash \)

2. set of MSCs is closed under \( \models_{df} \)
Complexity of safe realisability

Theorem: [Alur et al., 2001]
The decision problem “is a given set of MSCs safely realisable?” is in P.

Proof (sketch)
1. For a given finite set of MSCs, safe realisability can be checked in time $O((n^2 + r) \cdot k)$ where $k$ is the number of processes, $n$ the number of MSCs, and $r$ the number of events in all MSCs together.

2. If the MSCs are not safely realisable, the algorithm returns an MSC which is implied, but not included in the input set of MSCs. (We skip the details in this lecture.)