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

   set of MSCs

   $L \models w$

   MSC

2. Closure and inference revisited

3. Characterisation and complexity of safe realisability

   sufficient and necessary condition

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 $\mathcal{A}$ such that $\mathcal{L}(\mathcal{A})$ 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? or: to check realisability?
3. If so, how do such algorithms work?

Problem variants (1)

Realisability problem

INPUT: a set of MSCs

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

inputs

Different forms of requirements

* • Consider finite sets of MSCs, given as an enumerated set. $\{M_1, \ldots, M_k\}$
- 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 $\mathcal{A}$ such that $\mathcal{L}(\mathcal{A})$ equals the set of input MSCs.

outputs

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. $\forall$-bounded $\exists$-bounded
- ......

Today's lecture

Today's setting

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

no sync data
+ simpler accep-
tance condition

$$F = \prod_{p \in P} F_p$$

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.

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.

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

sufficient + necessary

safe

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.

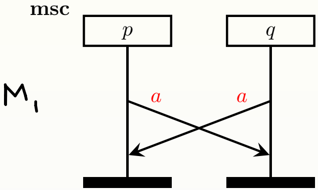
This is known as safe realisability.

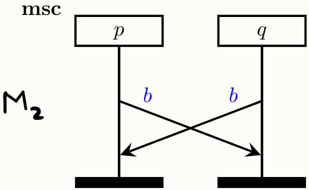
This is the setting of the previous lecture, but now focusing on deadlock-free CFMs

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.)

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



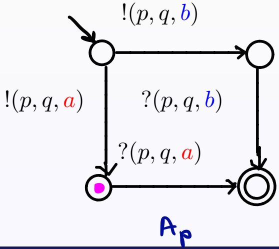


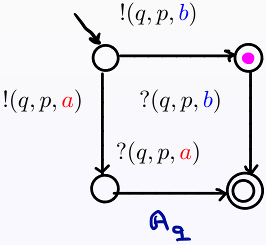
process p and q have to agree on either a or b

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

realisable

not safe realisable





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 $\underline{L = Lin(\mathcal{A})}$ for some <u>deadlock-free</u> CFM $\mathcal{A}$.

Note:

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

Overview

Weak closure

Definition (Inference relation and closure)

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

$$L \models w \quad \text{iff} \quad (\forall p \in \mathcal{P}.\, \exists v \in L.\, w \upharpoonright p = v \upharpoonright p)$$

Language L is closed under $\models$ whenever for every $w \in Act^*$, it holds: $L \models w$ implies $w \in L$.

allows

p_1 : $w \upharpoonright p_1 = v \upharpoonright p_1$

p_2 : $w \upharpoonright p_2 = u \upharpoonright p_2$

$v \neq u$

Weak closure

Definition (Inference relation and closure)

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

$$L \models w \quad \text{iff} \quad (\forall p \in \mathcal{P}.\, \exists v \in L.\, w \restriction p = v \restriction p)$$

Language L is closed under $\models$ whenever for every $w \in Act^*$, it holds: $L \models w$ implies $w \in L$.

L is closed under $\models$ $\not\longleftrightarrow$ L is weakly closed under $\models$

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 $w \in Act^*$.

Deadlock-free closure

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

Definition ((Deadlock-free) Inference relation)

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

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

proper word w

Deadlock-free closure

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

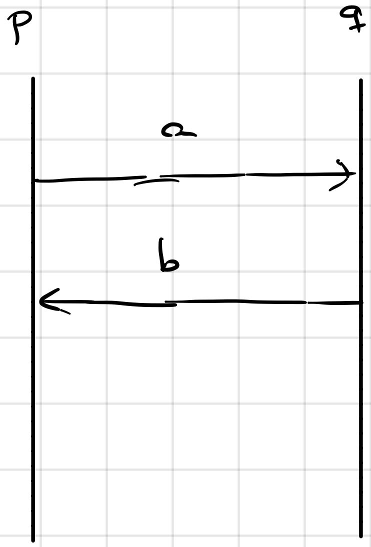
Definition ((Deadlock-free) Inference relation)

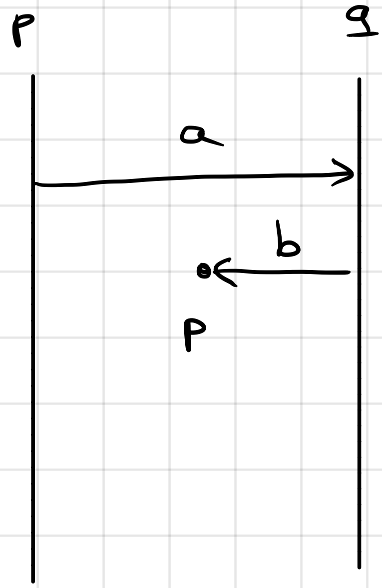
For well-formed $L \subseteq Act^*$, and proper word $w \in Act^*$, i.e., w is a prefix of a well-formed word, let:

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

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

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





partial MSC

Deadlock-free closure

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

Definition ((Deadlock-free) Inference relation)

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

$$L \models^{df} w \quad \text{iff} \quad (\forall p \in \mathcal{P}.\, \exists \underbrace{v \in pref(L)}_{\text{partial MSC}}.\, w \restriction p \underbrace{\text{ is a prefix of } v \restriction p}_{\text{partial}})$$

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

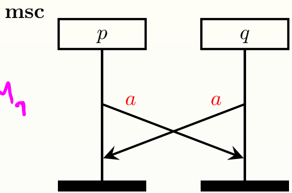
Language L is closed under $\models^{df}$ whenever $L \models^{df} w$ implies $w \in pref(L)$.

Intuition

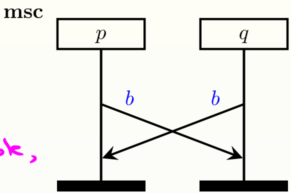
The closure condition asserts that the set of partial MSCs (i.e., prefixes of L) can be constructed from the projections of the MSCs in L onto individual processes.

Example

M_1



not safe realisable, realisable



M_2

Example

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

$L \models^{df} w$ but $w \notin pref(L)$

$$w \;=\; !(p,q,a)!(q,p,b) \notin pref(L)$$

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

$u = !(p,q,a)\,!(q,p,a)\,?(q,p,a)\,?(p,q,a)$

Note that L is closed under $\models$. So this shows that closure under $\models$ does not imply closure under $\models^{df}$

Deadlock-free weak CFM are closed under $\models^{df}$

Lemma:

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

Proof.

Similar proof strategy as for the closure of weak CFMs under $\models$ (see ~~previous~~ lecture).

9

Deadlock-free weak CFM are closed under $\models^{df}$

Lemma:

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

Proof.

Similar proof strategy as for the closure of weak CFMs under $\models$ (see previous lecture). Basic intuition is that if $w \upharpoonright p$ is a prefix of $v^p \upharpoonright p$, 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. $\square$

Overview

Characterisation of safe realisability

Theorem: [Alur *et al.*, 2001]

$L \subseteq Act^*$ is safely realisable iff L is $\underbrace{\text{weakly closed under} \models}_{1}$ $\underbrace{\text{and closed under} \models^{df}}_{2}$.

sufficient + necessary condition

closure under $\models$ for all well-formed prefixes of L

Characterisation of safe realisability

Theorem: [Alur *et al.*, 2001]

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

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 $\models^{df}$.

"$\Leftarrow$": Assume L is weakly closed under $\models$, and L is closed under $\models^{df}$. Let $L_p = \{ w \upharpoonright p \mid w \in L \}$, 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}^{p} 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.

$\boxed{\text{Now let CFM } \mathcal{A} = \left((A_p)_{p \in P}, s_{init}, F \right) \text{ with } s_{init} = \prod_{p \in P} s_{init}^{p} \text{ and } F = \prod_{p \in P} F_p .}$

<u>Claim</u>: (1) $L_{in}(\mathcal{A}) = L$ and (2) CFM $\mathcal{A}$ is deadlock-free.

(Obviously, then L is safe realisable).

<u>Proof</u>:

(1) "$\supseteq$": let $w \in L$. Then for every p, $w \upharpoonright p \in L_p$. Thus DFA A_p has an accepting run on $w \upharpoonright p$, and as $F = \prod_{p \in P} F_p$, CFM $\mathcal{A}$ has an accepting run on w.

"$\subseteq$": let $w \in Lin(A)$. As $Lin(A)$ is well-formed, w is well-formed. Since $F = \prod_p F_p$, it follows $w \upharpoonright p \in L_p$ for each process p. Thus $L \models w$. Since L is weakly closed under $\models$, and w is well-formed, it follow $w \in L$.

(2) A is deadlock free. This is proven as follows.

Assume A has read the input word $w \in Act^*$. 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 $w \upharpoonright p$ is a prefix of a word in L_p, for every process p. Since L is closed under $\models^{df}$, it follows that $w \in pref(L)$.

Let $w.u \in L$ for $u \neq \varepsilon$. As A_p is deterministic, it has a unique (local) accepting run for $(w.u) \upharpoonright p$.

This applies to every process p. As $F = \prod_p F_p$, it follows that CFM A has a unique accepting run for $w.u$. As this applies to every w, it follows that A is deadlock-free $\boxtimes$

Characterisation of safe realisability

Theorem: [Alur *et al.*, 2001]

$L \subseteq Act^*$ is safely realisable iff L is weakly closed under $\models$ 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 $\underbrace{\bigcup_{i=1}^{n} Lin(M_i) \text{ is closed under } \models \text{ and } \models^{df}}_{\text{weakly closed under } \models, \text{ closed under } \models^{df}}$.

Characterisation of safe realisability

Theorem realisability

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

L is regular and closed under $\models$
if and only if
$L = Lin(\mathcal{A})$ for some $\forall$-bounded weak CFM $\mathcal{A}$.

Theorem safe realisability

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

L is regular, weakly closed under $\models$ and closed under $\models^{df}$
if and only if
$L = Lin(\mathcal{A})$ for some $\forall$-bounded deadlock-free weak CFM $\mathcal{A}$.

Complexity of safe realisability

finite

Theorem: [Alur *et al.*, 2001]

The decision problem "is a given set of MSCs safely realisable?" is in P.

1. set of MSCs is weakly closed under $\models$

2. set of MSCs is closed under $\models^{df}$

Complexity of safe realisability

checking realisability is coNP-complete

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 $\mathcal{O}((n^2 + r) \cdot k)$ 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.)

is inferred