Foundations of the UML

Lecture 8+9: Realisability

Joost-Pieter Katoen

Lehrstuhl für Informatik 2
Software Modeling and Verification Group

http://moves.rwth-aachen.de/i2/370

23. November 2009

What is realisability?

Definition (Realisability)

1. MSC M is realisable whenever $\{M\} = L(\mathcal{A})$ for some CFM $\mathcal{A}$.
2. A finite set $\{M_1, \ldots, M_n\}$ of MSCs is realisable whenever $\{M_1, \ldots, M_n\} = L(\mathcal{A})$ for some CFM $\mathcal{A}$.
3. MSG G is realisable whenever $L(G) = L(\mathcal{A})$ for some CFM $\mathcal{A}$.

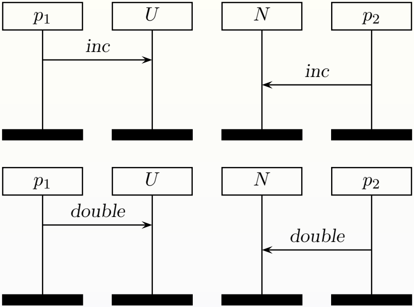
Alternatively

1. MSC M is realisable whenever $Lin(M) = Lin(\mathcal{A})$ for some CFM $\mathcal{A}$.
2. Set $\{M_1, \ldots, M_n\}$ of MSCs is realisable whenever $\bigcup_{i=1}^{n} Lin(M_i) = Lin(\mathcal{A})$ for some CFM $\mathcal{A}$.
3. MSG G is realisable whenever $Lin(G) = Lin(\mathcal{A})$ for some CFM $\mathcal{A}$.

We will consider realisability using its characterisation by linearisations.

Two example MSCs

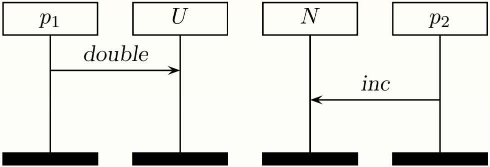
Consider the MSCs M_{inc} (left) and M_{db} (right):



Intuition

In M_{inc}, the volume of U (uranium) and N (nitric acid) is increased by one unit; in M_{db} both volumes are doubled. For safety reasons, it is essential that both ingredients are increased by the same amount!

A third, unavoidable fatal scenario



So:

The set $\{ M_{inc}, M_{db} \}$ is not realisable, as any CFM that realises this set also realises the inferred MSC M_{bad} above.

Note that:

Either of the MSCs M_{inc} or M_{db} alone does not imply M_{bad}.

Inference

Definition (Inference)

The set L of MSCs is said to infer MSC $M \notin L$ if and only if:

$$\text{for any CFM } \mathcal{A}.\, L \subseteq L(\mathcal{A}) \text{ implies } M \in L(\mathcal{A}).$$

Definition (Realisability)

The set L of MSCs is realisable iff L contains all MSCs that infers.

Intuition

A realisable MSC contains all its implied scenarios.

For computational purposes, an alternative characterisation is required.

Projection

Definition (Projection)

1. For MSC M and process p let $M \upharpoonright p$, the projection of M on process p, be the ordered sequence of actions occurring at process p in M.
2. For word $w \in Act^*$ and process p, the projection of w on process p, denoted $w \upharpoonright p$, is defined by:

$$\begin{array}{rcl} \epsilon \upharpoonright p & = & \epsilon \\ (!(r,q,a) \cdot w) \upharpoonright p & = & \begin{cases} !(r,q,a) \cdot (w \upharpoonright p) & \text{if } r = p \\ w \upharpoonright p & \text{otherwise} \end{cases} \end{array}$$

and similarly for receive actions.

Example

$w =$

$!(1,2,\text{req})!(1,2,\text{req})?(2,1,\text{req})!(2,1,\text{ack})?(2,1,\text{req})!(2,1,\text{ack})?(1,2,\text{ack})!(1,2,\text{req})$

$w \upharpoonright 1 = !(1,2,\text{req})!(1,2,\text{req})?(1,2,\text{ack})!(1,2,\text{req})$

Closure

Definition (Inference relation)

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

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

Definition (Closure under $\models$)

Language L is closed under $\models$ whenever $L \models w$ implies $w \in L$.

Intuition

The closure condition says that the set of MSCs (or, equivalently, well-formed words) can be obtained from the projections of the MSCs in L onto individual processes.

Closure: example

Example

$L = Lin(\{M_{up}, M_{db}\})$ is not closed under $\models$:

$$w = !(p_1, U, double)?(U, p_1, double)!(p2, N, inc)?(N, p_2, inc) \notin L$$

But: $L \models w$ since

- for process p_1, there is $u \in L$ with $w \upharpoonright p_1 = !(p_1, U, double) = u \upharpoonright p_1$, and
- for process p_2, there is $v \in L$ with $w \upharpoonright p_2 = !(p2, N, inc) = v \upharpoonright p_2$, and
- similar holds for processes U and N.

Weak CFMs

Definition (Weak CFM)

CFM $\mathcal{A} = (((S_p, \Delta_p))_{p \in \mathcal{P}}, \mathbb{D}, s_{init}, F)$ is weak if $\mathbb{D}$ is a singleton set.

Intuition

A weak CFM can be considered as CFM without synchronisation messages. (Therefore, the component $\mathbb{D}$ may be omitted.) For simplicity, today we address realisability with the aim of using weak CFMs as implementation.

Realisability revisited

A finite set $\{M_1, \ldots, M_n\}$ of MSCs is realisable whenever $\{ M_1, \ldots, M_n\} = L(\mathcal{A})$ for some weak CFM $\mathcal{A}$

Weak CFMs are closed under $\models$

Lemma:

For any weak CFM $\mathcal{A}$, $Lin(\mathcal{A})$ is closed under $\models$.

Proof

Let $\mathcal{A}$ be a weak CFM. Since $\mathcal{A}$ is a CFM, any $w \in Lin(\mathcal{A})$ is well-formed.
Let $w \in Act^*$ be well-formed and assume $Lin(\mathcal{A}) \models w$.
To show that $Lin(\mathcal{A})$ is closed under $\models$, we prove that $w \in Lin(\mathcal{A})$.
By definition of $\models$, for any process p there is $v^p \in Lin(\mathcal{A})$ with $v^p \upharpoonright p = w \upharpoonright p$.
Let π be an accepting run of $\mathcal{A}$ on v^p and let run $\pi \upharpoonright p$ visit only states of $\mathcal{A}_p$ while taking only transitions in Δ_p. Then, $\pi \upharpoonright p$ is an accepting run of "local" automaton $\mathcal{A}_p$ on the word $v^p \upharpoonright p = w \upharpoonright p$.
The "local" accepting runs $\pi \upharpoonright p$ for all processes p together can be combined to obtain an accepting run of $\mathcal{A}$ on w.
Thus, $w \in Lin(\mathcal{A})$. □

Characterisation of realisability

Theorem: [Alur et al., 2001]

$L \subseteq Act^*$ is realisable iff L is closed under $\models$.

Proof

On the black board.

Corollary

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

Characterisation of realisability

Theorem

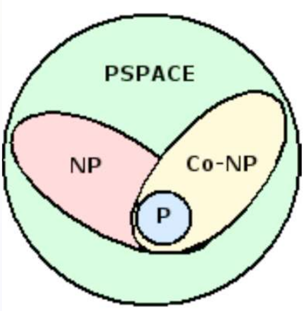
For any well-formed $L \subseteq Act^*$:

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

Complexity of realisability

Let co-NP be the class of all decision problems C with $\overline{C}$, the complement of C, is in NP.

A problem C is co-NP complete if it is in co-NP, and it is co-NP hard, i.e., each for any co-NP problem there is a polynomial reduction to C.



Complexity of realisability

Theorem: [Alur et al., 2001]

The decision problem "is a given set of MSCs realisable?" is co-NP complete.

Proof

1. Membership in co-NP is proven by showing that its complement is in NP. This is rather standard.
2. The co-NP hardness proof is based on a polynomial reduction of the join dependency problem to the above realisability problem. (Details on the black board.)

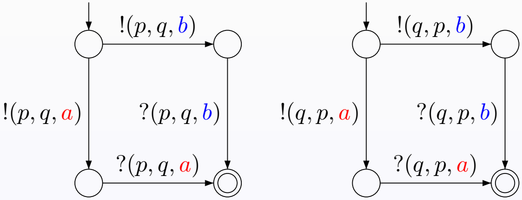
RWTH AACHEN UNIVERSITY

Safe realisability

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 $\{ M_1, M_2 \}$:



process p process q

Deadlock occurs when, e.g., p sends a and q sends b

Safe realisability

Definition (Safe realisability)

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

Consider 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.

Closure revisited

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

Definition (Inference relation, revisited)

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

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

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

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

Intuition

The closure condition says 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 weak CFM are closed under $\models^{df}$

Lemma:

For any 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 $\models$. 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 the 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.

Example

Example

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

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

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

Characterisation of safe realisability

Theorem: [Alur et al., 2001]

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

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 $\models^{df}$.

RWTH AACHEN UNIVERSITY

Characterisation of safe realisability

Theorem

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

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

RWTH AACHEN UNIVERSITY

Complexity of safe realisability

Theorem: [Alur et al., 2001]

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

Proof

1. For a given finite set of MSCs, safe realisability can be checked in time $\mathcal{O}((k^2 + r) \cdot n)$ where n is the number of processes, k 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.

(Details on the black board.)