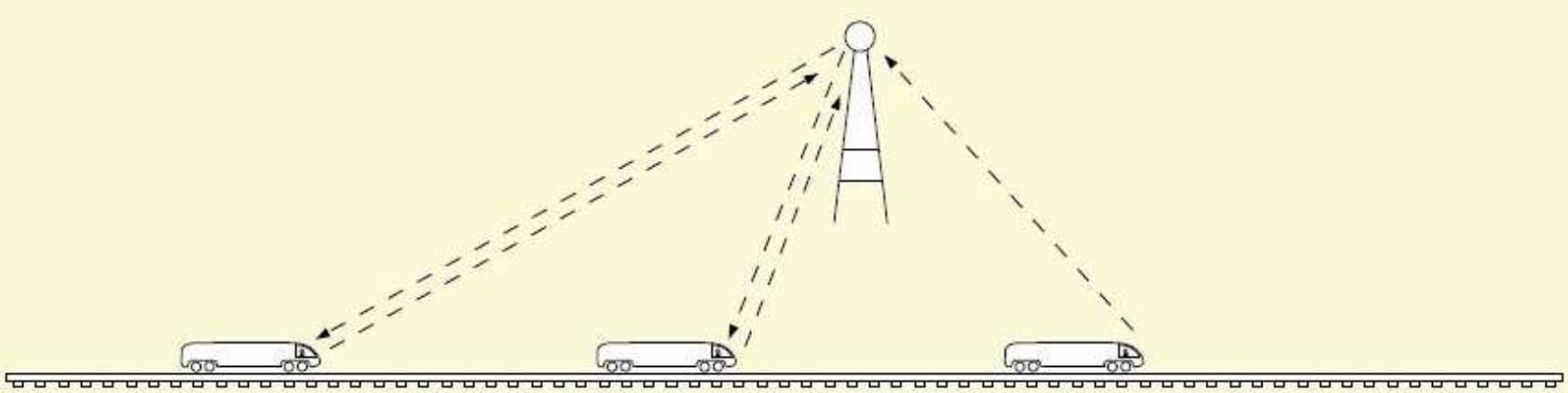
Applications of Hierarchical Reasoning in the Verification of Complex Systems

Swen Jacobs and Viorica Sofronie-Stokkermans

MPI für Informatik
Saarbrücken, Germany

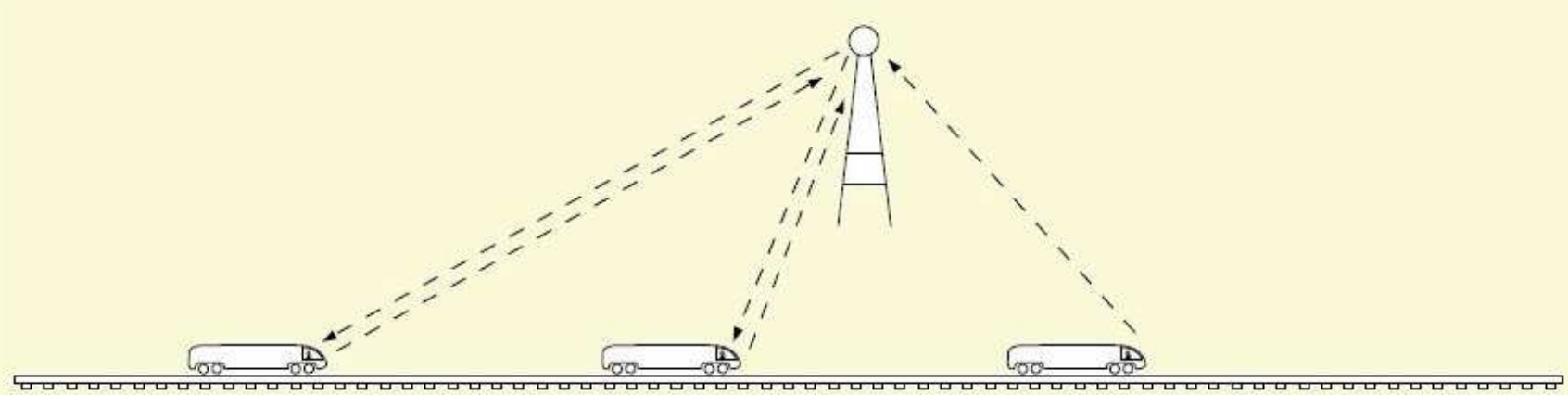
Pragmatics of Decision Procedures in Automated Reasoning
FLoC / IJCAR 2006
August 21 2006

Case Study: European Train Control System



- Existing approaches $\longrightarrow$ problems
- Symbolic approach $\longrightarrow$ problems
- Idea

Modelling the ETCS Case Study



Model the behaviour of an undefined number of trains on a track:

Update rules $\mathcal{K}(pos, pos')$: relation of $pos(i)$ and $pos'(i)$

Property of positions:

$Mon(pos): \quad \forall i, j: \; 0 \leq i < j < n \rightarrow pos(i) > pos(j)$

To prove: $\mathcal{T} \cup \mathcal{K}(pos, pos') \cup Mon(pos) \models Mon(pos')$

Our Idea

Given the axiom $\forall i, j: \ 0 \leq i < j < n \rightarrow pos(i) > pos(j)$,
we want to prove unsatisfiability of
$\neg Mon(pos): \quad 0 \leq a < b < n \wedge pos(a) \leq pos(b)$.

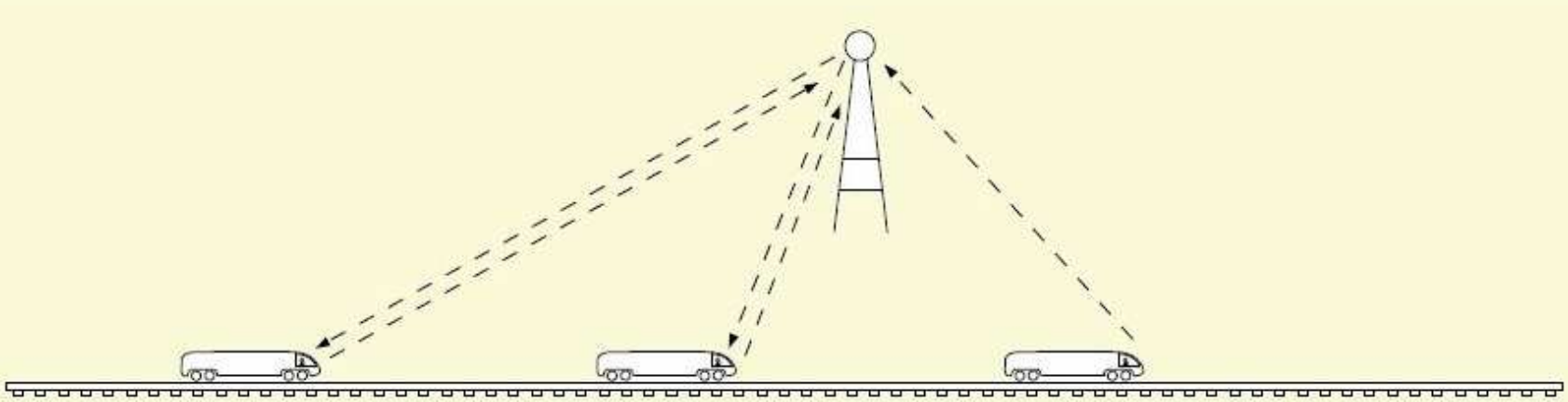
To do this, only consider instances
$0 \leq a < b < n \rightarrow pos(a) \leq pos(b)$ and
$0 \leq b < a < n \rightarrow pos(b) \leq pos(a)$ of the axiom.

Furthermore, we can eliminate function symbol pos and let a solver for the base theory decide satisfiability.

Structure

0. Introduction
1. Case Study
2. Applying Hierarchical Reasoning
3. Conclusion and Outlook

Modelling the ETCS Case Study



- Train positions before and after update: $pos(i), pos'(i)$
- Time between updates: $\Delta t > 0$
- Minimum and maximum speed of trains: $\min < \max$
- Minimum secure distance: l_{alarm}
- Number of trains: $n > 0$

Modelling the ETCS Case Study

Simple axiomatization $\mathcal{K}(pos, pos')$ of updates:

$$\forall i\ (i = 0 \rightarrow pos(i) + \Delta t{*}\mathsf{min} \leq pos'(i) \leq pos(i) + \Delta t{*}\mathsf{max})$$

$$\forall i\ (0 < i < n\ \wedge\ pos(i-1) > 0\ \wedge\ pos(i-1) - pos(i) \geq l_{\mathsf{alarm}} \rightarrow pos(i) + \Delta t{*}\mathsf{min} \leq pos'(i) \leq pos(i) + \Delta t{*}\mathsf{max})$$

$$\forall i\ (0 < i < n\ \wedge\ pos(i-1) > 0\ \wedge\ pos(i-1) - pos(i) < l_{\mathsf{alarm}} \rightarrow pos'(i) = pos(i) + \Delta t{*}\mathsf{min})$$

$$\forall i\ (0 < i < n\ \wedge\ pos(i-1) \leq 0\ \rightarrow\ pos'(i) = pos(i))$$

Local Theory Extensions

Theory Extensions: If $\mathcal{T}_0$ is a theory, $\mathcal{K}$ a set of clauses with new function symbols, then $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$ is a theory extension.

Locality: A theory extension is local if for deciding satisfiability of a ground goal G, we only need to consider instances of $\mathcal{K}$ with ground extension terms that appear in G or $\mathcal{K}$.

Verification of the Case Study

Verification Task: Given the base theory $\mathbb{R} \cup \mathcal{I}$ and $Mon(pos)$, prove that pos' (defined by $\mathcal{K}(pos, pos')$) is still monotone:

$$\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos') \cup \neg Mon(pos') \models \bot$$

Approach: Chain of extensions

$$\mathbb{R} \cup \mathcal{I} \subseteq \mathbb{R} \cup \mathcal{I} \cup Mon(pos) \subseteq \mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$$

Proof steps:

- Show that both extensions are local
- Reduce problem from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$ to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$
- Reduce problem from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$ to $\mathbb{R} \cup \mathcal{I}$

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup \mathit{Mon}(\mathit{pos}) \cup \mathcal{K}(\mathit{pos}, \mathit{pos}')$

to $\mathbb{R} \cup \mathcal{I} \cup \mathit{Mon}(\mathit{pos})$

wrt. $G = \neg \mathit{Mon}(\mathit{pos}') = \{0 \leq a < b < n, \mathit{pos}'(a) \leq \mathit{pos}'(b)\}$:

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$

to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$

wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$:

1. Take instances of axioms in $\mathcal{K}(pos, pos')$ wrt. G

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$

to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$

wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$:

1. Take instances of axioms in $\mathcal{K}(pos, pos')$ wrt. G, e.g.

$$\forall i\ (0 < i < n\ \wedge\ pos(i-1) > 0\ \wedge\ pos(i-1) - pos(i) \geq l_{\text{alarm}} \\ \rightarrow pos(i) + \Delta t * \min \leq pos'(i) \leq pos(i) + \Delta t * \max)$$

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$

to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$

wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$:

1. Take instances of axioms in $\mathcal{K}(pos, pos')$ wrt. G, e.g.

$$\forall i\ (0 < i < n\ \wedge\ pos(i-1) > 0\ \wedge\ pos(i-1) - pos(i) \geq l_{\text{alarm}} \rightarrow pos(i) + \Delta t * \min \leq pos'(i) \leq pos(i) + \Delta t * \max)$$

$$0 < a < n\ \wedge\ pos(a-1) > 0\ \wedge\ pos(a-1) - pos(a) \geq l_{\text{alarm}} \rightarrow pos(a) + \Delta t * \min \leq pos'(a) \leq pos(a) + \Delta t * \max,$$

$$0 < b < n\ \wedge\ pos(b-1) > 0\ \wedge\ pos(b-1) - pos(b) \geq l_{\text{alarm}} \rightarrow pos(b) + \Delta t * \min \leq pos'(b) \leq pos(b) + \Delta t * \max$$

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$

to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$

wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$:

1. Take instances of axioms in $\mathcal{K}(pos, pos')$ wrt. $G \Rightarrow \mathcal{K}[G]$

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$

to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$

wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$:

1. Take instances of axioms in $\mathcal{K}(pos, pos')$ wrt. $G \Rightarrow \mathcal{K}[G]$
2. Purify $\mathcal{K}[G]$ and G wrt. pos'

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$

to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$

wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$:

1. Take instances of axioms in $\mathcal{K}(pos, pos')$ wrt. $G \Rightarrow \mathcal{K}[G]$
2. Purify $\mathcal{K}[G]$ and G wrt. pos', e.g.

$$0 < a < n \wedge pos(a-1) > 0 \wedge pos(a-1) - pos(a) \geq l_{\text{alarm}}$$
$$\rightarrow pos(a) + \Delta t * \min \leq pos'(a) \leq pos(a) + \Delta t * \max$$

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$

to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$

wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$:

1. Take instances of axioms in $\mathcal{K}(pos, pos')$ wrt. $G \Rightarrow \mathcal{K}[G]$
2. Purify $\mathcal{K}[G]$ and G wrt. pos', e.g.

$$0 < a < n \wedge pos(a-1) > 0 \wedge pos(a-1) - pos(a) \geq l_{\text{alarm}}$$
$$\rightarrow pos(a) + \Delta t * \min \leq c_1 \leq pos(a) + \Delta t * \max$$

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$
to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$
wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$:

1. Take instances of axioms in $\mathcal{K}(pos, pos')$ wrt. $G \Rightarrow \mathcal{K}[G]$
2. Purify $\mathcal{K}[G]$ and G wrt. pos', e.g.

$$0 < a < n \wedge pos(a-1) > 0 \wedge pos(a-1) - pos(a) \geq l_{\text{alarm}}$$
$$\rightarrow pos(a) + \Delta t * \min \leq c_1 \leq pos(a) + \Delta t * \max$$

D: $c_1 = pos'(a)$

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$

to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$

wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$:

1. Take instances of axioms in $\mathcal{K}(pos, pos')$ wrt. $G \Rightarrow \mathcal{K}[G]$
2. Purify $\mathcal{K}[G]$ and G wrt. $pos' \Rightarrow \mathcal{K}_0 \wedge G_0 \wedge D$

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$
to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$
wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$:

1. Take instances of axioms in $\mathcal{K}(pos, pos')$ wrt. $G \Rightarrow \mathcal{K}[G]$
2. Purify $\mathcal{K}[G]$ and G wrt. $pos' \Rightarrow \mathcal{K}_0 \wedge G_0 \wedge D$
3. Reduce to satisfiability in $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$:

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$

to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$

wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$:

1. Take instances of axioms in $\mathcal{K}(pos, pos')$ wrt. $G \Rightarrow \mathcal{K}[G]$
2. Purify $\mathcal{K}[G]$ and G wrt. $pos' \Rightarrow \mathcal{K}_0 \wedge G_0 \wedge D$
3. Reduce to satisfiability in $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$:

   D: $c_1 = pos'(a), c_2 = pos'(b)$

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$
to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$
wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$:

1. Take instances of axioms in $\mathcal{K}(pos, pos')$ wrt. $G \Rightarrow \mathcal{K}[G]$
2. Purify $\mathcal{K}[G]$ and G wrt. $pos' \Rightarrow \mathcal{K}_0 \wedge G_0 \wedge D$
3. Reduce to satisfiability in $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$:

   D: $c_1 = pos'(a), c_2 = pos'(b)$
   N: $a = b \rightarrow c_1 = c_2$

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$
to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$
wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$:

1. Take instances of axioms in $\mathcal{K}(pos, pos')$ wrt. $G \Rightarrow \mathcal{K}[G]$
2. Purify $\mathcal{K}[G]$ and G wrt. $pos' \Rightarrow \mathcal{K}_0 \wedge G_0 \wedge D$
3. Reduce to satisfiability in $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$:
   $\mathcal{K}_0 \wedge G_0 \wedge N$ satisfiable in $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$
   $\Leftrightarrow$
   G satisfiable in $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$

to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$

wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$

$\Rightarrow \mathcal{K}_0 \wedge G_0 \wedge N = G'$

$$
\begin{aligned}
G' = \quad & \mathcal{K}(pos, pos')[a/i, c_1/pos'(i)] \\
& \wedge \mathcal{K}(pos, pos')[b/i, c_2/pos'(i)] \\
& \wedge \{0 \leq a < b < n, c_1 \leq c_2\} \\
& \wedge \{a = b \rightarrow c_1 = c_2\}
\end{aligned}
$$

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$
to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$
wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$
$\Rightarrow \mathcal{K}_0 \wedge G_0 \wedge N = G'$

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$ to $\mathbb{R} \cup \mathcal{I}$ wrt. G':

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$
to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$
wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$
$\Rightarrow \mathcal{K}_0 \wedge G_0 \wedge N = G'$

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$ to $\mathbb{R} \cup \mathcal{I}$ wrt. G':

1. Take instances of $Mon(pos)$ wrt. $G' \Rightarrow Mon(pos)[G']$

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$
to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$
wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$
$\Rightarrow \mathcal{K}_0 \wedge G_0 \wedge N = G'$

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$ to $\mathbb{R} \cup \mathcal{I}$ wrt. G':

1. Take instances of $Mon(pos)$ wrt. $G' \Rightarrow Mon(pos)[G']$
2. Purify $Mon(pos)[G']$ and G' wrt. $pos \Rightarrow Mon(pos)_0 \wedge G'_0 \wedge D'$

Proof Steps

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos) \cup \mathcal{K}(pos, pos')$
to $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$
wrt. $G = \neg Mon(pos') = \{0 \leq a < b < n, pos'(a) \leq pos'(b)\}$
$\Rightarrow \mathcal{K}_0 \wedge G_0 \wedge N = G'$

Reduction from $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$ to $\mathbb{R} \cup \mathcal{I}$ wrt. G':

1. Take instances of $Mon(pos)$ wrt. $G' \Rightarrow Mon(pos)[G']$
2. Purify $Mon(pos)[G']$ and G' wrt. $pos \Rightarrow Mon(pos)_0 \wedge G'_0 \wedge D'$
3. Reduce to satisfiability in $\mathbb{R} \cup \mathcal{I}$:
   $Mon(pos)_0 \wedge G'_0 \wedge N'$ satisfiable in $\mathbb{R} \cup \mathcal{I}$
   $\Leftrightarrow$
   G' satisfiable in $\mathbb{R} \cup \mathcal{I} \cup Mon(pos)$

Extensions of Case Study

Approach was extended in several ways:

- Consider an axiomatization that allows incoming and leaving trains
- Consider a safety property that takes into account length of trains
- Multiple extensions with sets of axioms $\mathcal{K}(pos_i, pos_{i+1})$ allow for bounded model checking

Conclusion

- Hierarchical reasoning gives a decision procedure for verifying properties of certain parametrized systems
- Reasoning about these systems can be reduced to a decidable base theory
- We can even determine constraints between parameters s.t. safety conditions are guaranteed

Future Work

- Extend results to more complex systems
- Identify classes of systems that can be described by chains of local extensions
- Obtain general decidability results (not restricted to verification)

Thanks

Thanks to Johannes Faber (Univ. Oldenburg) for example

Thanks to you for listening!

AVACS Project: ETCS Case Study

More complex axiomatization (allows incoming and leaving trains):

(V1-V4) similar to F1 to F4, except for upper and lower bound

(V5) $\mathsf{last} - \mathsf{first} + 1 < \mathsf{maxTrains} \rightarrow \mathsf{last}' = \mathsf{last} \vee \mathsf{last}' = \mathsf{last} + 1$

(V6) $\mathsf{last} - \mathsf{first} + 1 = \mathsf{maxTrains} \rightarrow \mathsf{last}' = \mathsf{last}$

(V7) $\mathsf{last} - \mathsf{first} + 1 > 0 \rightarrow \mathsf{first}' = \mathsf{first} \vee \mathsf{first}' = \mathsf{first} + 1$

(V8) $\mathsf{last} - \mathsf{first} + 1 = 0 \rightarrow \mathsf{first}' = \mathsf{first}$

(V9) $\mathsf{last}' = \mathsf{last} + 1 \quad \rightarrow \quad \mathit{pos}'(\mathsf{last}') < \mathit{pos}'(\mathsf{last})$

can also be proven local, invariants can be handled in same way.

AVACS Project: ETCS Case Study

More complex verification condition (considers length of trains):

$$\forall i, j, k: \ \mathit{first} \leq j \leq i \leq \mathit{last} \ \wedge \ i - j = k \\ \rightarrow \mathit{pos}(j) - \mathit{pos}(i) \geq k * \mathsf{LengthTrain}$$