Appendix to “Reachability Analysis in Verification via Supercompilation”

Alexei Lisitsa\(^1\) and Andrei P. Nemytkh\(^2\)

\(^1\) Department of Computer Science, The University of Liverpool
alexei@csc.liv.ac.uk

\(^2\) Program Systems Institute of Russian Academy of Sciences
nemytykh@math.botik.ru

Abstract. This document is an appendix to our paper “Reachability Analysis in Verification via Supercompilation”. We feel ourselves free to refer to the sections of the indicated paper [25].

Keywords: Program verification, cache coherence protocols, program specialization, supercompilation.

1 Appendix. Example: MOESI protocol

In this section we apply the parameterized testing (described in Section [Parameterized Testing]) to the MOESI cache coherence protocol considered in [5]. We will work in terms of \(A(V,F)\). G. Delzanno [5] describes evolution of this protocol as follows:

\[(rh)\] modified + owned + shared + exclusive \(\geq 1 \rightarrow \).

\[(rm)\] invalid \(\geq 1 \rightarrow \)
\[\text{invalid}' = \text{invalid} - 1, \text{exclusive}' = 0, \text{modified}' = 0, \text{shared}' = \text{shared} + \text{exclusive} + 1, \text{owned}' = \text{owned} + \text{modified} .\]

\[(wh1)\] modified \(\geq 1 \rightarrow \).

\[(wh2)\] exclusive \(\geq 1 \rightarrow \)
\[\text{exclusive}' = \text{exclusive} - 1, \text{modified}' = \text{modified} + 1 .\]

\[(wh3)\] shared + owned \(\geq 1 \rightarrow \text{exclusive}' = 1, \text{shared}' = 0, \text{modified}' = 0, \text{owned}' = 0, \text{invalid}' = \text{invalid} + \text{exclusive} + \text{modified} + \text{owned} + \text{shared} - 1.\]

\[(wm)\] invalid \(\geq 1 \rightarrow \text{exclusive}' = 1, \text{shared}' = 0, \text{modified}' = 0, \text{owned}' = 0, \text{invalid}' = \text{invalid} + \text{exclusive} + \text{modified} + \text{owned} + \text{shared} - 1 .\]

The start configuration of the protocol is parameterized with \(x\) ranged over natural numbers:

\[\text{invalid} = x + 1, \text{modified} = \text{shared} = \text{exclusive} = \text{owned} = 0.\]

Correctness of the protocol is expressed with unreachable of configurations of the following form:

\[-(C_1)\] exclusive + shared + owned \(\geq 1, \text{modified} \geq 1;\]
-- (C_2) exclusive $\geq 1$, shared + owned $\geq 1$;
-- (C_3) modified $\geq 2$;
-- (C_4) exclusive $\geq 2$.

The MOESI protocol is a kind of parameterized protocols. The specification of the protocol is an abstraction of an automata model of protocols. The variables count the number of the automatons being in the corresponding states. See [5] for the details.

1.1 An Interpreter of the MOESI Cache Coherence Protocol

The protocol can be considered as a non-deterministic dynamic system with discrete time, where the slots of the time are randomly labeled with the names of the actions developing the system. We model this dynamic system by adding an additional variable \(\text{time}\) and use the unary arithmetic: \(0 = \lambda, n + 1 = I n\).

Let \(\text{time}, \text{inv}, \text{mod}, \text{sh}, \text{exc}, \text{own}, \text{rm}, \text{wh2}, \text{wh3A}, \text{wh3B}, \text{wm}, I \in K\) and \(\text{Loop}\).

\(\text{RandomAction} \in \mathcal{F}_N\). Recall that \(e.\ldots \in \mathcal{E}\) and \(s.\ldots \in \mathcal{S}\), where \(\mathcal{E} \cup \mathcal{S} = \mathcal{V}\) (see the section \([A \text{ Free Monoid of Terms}]\)). The rules of the MOESI protocol are encoded in term of \(A(\mathcal{V}, \mathcal{F})\) as follows:

\[
\begin{align*}
<\text{RandomAction } \text{rm } (\text{inv } I \ e.x)(\text{mod } e.y)(\text{sh } e.z)(\text{exc } e.u)(\text{own } e.v)> &= (\text{inv } e.x)(\text{mod } ) (\text{sh } I \ e.z \ e.u)(\text{exc })(\text{own } e.y \ e.v); \\
<\text{RandomAction } \text{wh2 } (\text{inv } e.x)(\text{mod } e.y)(\text{sh } e.z)(\text{exc } I \ e.u)(\text{own } e.v)> &= (\text{inv } e.x)(\text{mod } I \ e.y)(\text{sh } e.z)(\text{exc } e.u)(\text{own } e.v); \\
<\text{RandomAction } \text{wh3A } (\text{inv } e.x)(\text{mod } e.y)(\text{sh } I \ e.z)(\text{exc } e.u)(\text{own } e.v)> &= (\text{inv } e.v \ e.u \ e.z \ e.y e.x)(\text{mod })(\text{sh })(\text{exc } I)(\text{own}); \\
<\text{RandomAction } \text{wh3B } (\text{inv } e.x)(\text{mod } e.y)(\text{sh } e.z)(\text{exc } e.u)(\text{own } I \ e.v)> &= (\text{inv } e.v \ e.u \ e.z \ e.y e.x)(\text{mod })(\text{sh })(\text{exc } I)(\text{own}); \\
<\text{RandomAction } \text{wm } (\text{inv } I \ e.x)(\text{mod } e.y)(\text{sh } e.z)(\text{exc } e.u)(\text{own } e.v)> &= (\text{inv } e.v \ e.u \ e.z \ e.y e.x)(\text{mod })(\text{sh })(\text{exc } I)(\text{own});
\end{align*}
\]

Here the first terms in the left sides of the rules correspond to the cases of the specification of the protocol. The \(\text{wh3}\) case is represented with two subcases: the first one is \(\text{shared } \geq 1\), the second is \(\text{owned } \geq 1\). We omit the trivial cases \(\text{rh}\) and \(\text{wh1}\). Recall that \((\text{sh } ) = (\text{sh } \lambda)\).

Evolution of the protocol during a given time is described with the following two rules:

\[
\begin{align*}
<\text{Loop } (\text{time } ) (\text{inv } e.x)(\text{mod } e.y)(\text{sh } e.z)(\text{exc } e.u)(\text{own } e.v)> &= (\text{inv } e.x)(\text{mod } e.y)(\text{sh } e.z)(\text{exc } e.u)(\text{own } e.v); \\
<\text{Loop } (\text{time } s.\ldots \text{e.t} ) (\text{inv } e.x)(\text{mod } e.y)(\text{sh } e.z)(\text{exc } e.u)(\text{own } e.v)> &= <\text{Loop } (\text{time } e.t) <\text{RandomAction } s.\ldots \text{s.tm } (\text{inv } e.x)(\text{mod } e.y)(\text{sh } e.z)(\text{exc } e.u)(\text{own } e.v)>>; \\
\end{align*}
\]

Developing of the system stops when the time is exhausted and the interpreter returns the final state of the system. The initial term of the term rewriting system is:

\[
\tau = <\text{Loop } (\text{time } e.t) (\text{inv } I \ e.x)(\text{mod } ) (\text{sh } )(\text{exc } ) (\text{own } )><
\]

The term parameterized with two parameters \(e.\text{time}\) and \(e.\text{x}\).
1.2 The Property of the MOESI Cache Coherence Protocol

The property of the protocol is defined with the following passive terms (see the section [Inductive Proofs of Safety Properties]):

\[ q_1 = (\text{inv } e.x)(\text{mod } I e.y)(\text{sh } I e.z)(\text{exc } e.u)(\text{own } e.v), \]
\[ q_2 = (\text{inv } e.x)(\text{mod } I e.y)(\text{sh } e.z)(\text{exc } I e.u)(\text{own } e.v), \]
\[ q_3 = (\text{inv } e.x)(\text{mod } e.y)(\text{sh } I e.z)(\text{exc } I e.u)(\text{own } e.v), \]
\[ q_4 = (\text{inv } e.x)(\text{mod } I e.y)(\text{sh } e.z)(\text{exc } I e.u)(\text{own } I e.v), \]
\[ q_5 = (\text{inv } e.x)(\text{mod } e.y)(\text{sh } I e.z)(\text{exc } e.u)(\text{own } I e.v), \]
\[ q_6 = (\text{inv } e.x)(\text{mod } I e.y)(\text{sh } e.z)(\text{exc } e.u)(\text{own } I e.v). \]

Where the terms \( q_1, q_2, q_3 \) correspond to the case \( (C_1) \), \( q_4, q_5 \) correspond to \( (C_2) \), \( q_6 \) to \( (C_3) \) and \( q_7 \) to \( (C_4) \).

1.3 The Inductive Proof

Let \( q \) be the set \( \bigcup_i \{ q_i \} \). Now we are ready to prove the safety property \( Q_q \) of the MOESI protocol with the rules defined in the section [Inductive Proofs of Safety Properties] and using the strategies described in the sections [Towards Effectiveness], [Restrictions on Term-rewriting Systems].

We use the same notations as in the example [Inductive Proofs of Safety Properties] and shorten the names Loop and RandomAction to L and R. We mark the vertices of the trees \( T_i \) with their creation times and underline the path starting in the root and ending in the vertex being considered. The main terms taking part in closing and generalization are given in the table 1. Given a tree \( T_{i+1} \), sometimes we will omit an upper part of the tree, which is the same as in \( T_i \).

Looking for generalization of the main statement START rule gives the tree \( T_0 \) containing the only initial vertex \( [\tau]^n \). UNFOLD rule yields

\[ a_2 = \langle \text{Let } e.h \text{ eq } \langle R s.m (\text{inv } e.x)(\text{mod})(\text{sh } I)(\text{exc})(\text{own}) \rangle \rangle \text{ in } \langle L \text{ (time } e.t) e.h \rangle \rangle \text{ in } [\tau]^n, \]

\[ ([\tau]^n \xrightarrow{a_1} (\tau)^n \xrightarrow{a_2}). \]

The passive term \( t_{a_1} \) does not match with \( q_i \) for any \( i \) and, hence, we close \( a_1 \). That is a basic case of the induction corresponding time = 0.

According the chosen strategy “call by value”, UNFOLD generates (from the cases rm, wm) \( T_2 = \{ [\tau]^n, ([\tau]^n \xrightarrow{a_1} (\tau)^n \xrightarrow{a_2}), (a_2^* \xrightarrow{b_2})(a_2^* \xrightarrow{b_2}), (a_2^* \xrightarrow{b_2}) \} \). See the table 1 for the terms \( b_{a}, b_{a} \).

There exist only two vertices on the path starting in the root and ending in the vertex \( a_2^* \) being considered. \( \tau \neq t_{a_2} \) holds. We unfold the term \( t_{a_2} \); \( T_3 = \{ \ldots, ([\tau]^n \xrightarrow{a_2^*} b_2), (a_2^* \xrightarrow{b_2}) \} \).
The passive term $t_{a_3}$ does not match with $q_i$ for any $i$, that causes we closed $a_1$. That is the second basic case of the induction corresponding time $= 1$. Below we omit the comments on the testing.

$
\tau \not\subseteq \text{t}_{b_3} \text{ and } t_{a_2} \not\subseteq \text{t}_{b_3} \text{ forbid to generalize } t_{b_3} \text{ and cause unfolding of } t_{d_5}.
$

We have $T_4 = \{ \ldots (a_2 \overset{e}{\rightarrow} b_3), (a_2 \overset{e}{\rightarrow} b_4), (b_3 \overset{e}{\rightarrow} d_5), (b_4 \overset{e}{\rightarrow} d_5), (c_3 \overset{e}{\rightarrow} d_5), (c_4 \overset{e}{\rightarrow} d_5) \}$. 

Here the new vertices were generated from the cases $\text{rm}$, $\text{wh3A}$, $\text{wm}$. There exists the only open vertex $c_0$ in $T_4$ and each of its ancestor $\not\subseteq t_{c_0}$. That forces us to unfold $t_{d_5}$ and the next tree is: $T_5 = \{ \ldots (b \overset{e}{\rightarrow} d_5), (d_5 \overset{e}{\rightarrow} d_5), (d_5 \overset{e}{\rightarrow} d_5), (d_5 \overset{e}{\rightarrow} d_5), (d_5 \overset{e}{\rightarrow} d_5) \}$. $c_{10} = [\langle \text{inv e.x)(mod)(sh I I)(exc)(own) \rangle^e \text{ in } <L (\text{time e.t) e.h}>]^a$, $(d_5 \overset{e}{\rightarrow} c_{10})]$. $c_{11} = [\langle \text{Let e.h eq <<R s.m (inv e.x)(mod)(sh I I)(exc)(own)>> in <L (\text{time e.t) e.h}>]^a$, $(c_{11} \overset{e}{\rightarrow} c_{10})]$. 

It is easy to see that there exists no another possibility for the open vertex $d_5$ but to take the vertex $b_3$, an ancestor of this vertex, and $t_{b_3} \not\subseteq t_{d_5}$ holds. GENERALIZE rule constructs the term $g_{b_3} = [\langle \text{time e.t) (inv e.x)(mod)(sh I e.z)(exc)(own)>\text{ in } <L (\text{time e.t) e.h}>]^a$, $(c_{11} \overset{e}{\rightarrow} c_{10})]$. $c_{12} = [\langle \text{inv e.x)(mod)(sh I e.z)(exc)(own)>\text{ in } <L (\text{time e.t) e.h}>]^a$, $(b_3 \overset{e}{\rightarrow} c_{12})]$. $c_{13} = [\langle \text{Let e.h eq <<R s.m (inv e.x)(mod)(sh I e.z)(exc)(own)>> in <L (\text{time e.t) e.h}>]^a$, $(c_{13} \overset{e}{\rightarrow} d_{13})]$. $\tau \not\subseteq g_{b_3} \text{ and } t_{a_2} \not\subseteq g_{b_3} \text{ forbid to generalize } g_{b_3} \text{ and cause unfolding of } t_{c_{13}}$. We have $T_6 = \{ \ldots (a_3 \overset{e}{\rightarrow} b_5), (a_3 \overset{e}{\rightarrow} b_4), (b_5 \overset{e}{\rightarrow} c_{12}), (b_4 \overset{e}{\rightarrow} c_{13}), (c_{13} \overset{e}{\rightarrow} d_{14}) \}$. Here the new vertices were generated from the cases $\text{rm}$, $\text{wh3A}$, $\text{wm}$. For any ancestor $[n]_{e}$ of the open vertex $c_{13}$ we have $\eta \not\subseteq t_{c_{13}}$. UNFOLD rule yields: $T_8 = \{ \ldots (b \overset{e}{\rightarrow} c_{13}), (c_{13} \overset{e}{\rightarrow} d_{14}), (c_{14} \overset{e}{\rightarrow} d_{15}), (c_{15} \overset{e}{\rightarrow} d_{16}) \}$ $c_{17} = [\langle \text{inv e.x)(mod)(sh I e.z)(exc)(own)>\text{ in } <L (\text{time e.t) e.h}>]^a$, $(d_{14} \overset{e}{\rightarrow} c_{17})]$. $c_{18} = [\langle \text{Let e.h eq <<R s.m (inv e.x)(mod)(sh I e.z)(exc)(own)>> in <L (\text{time e.t) e.h}>]^a$, $(d_{14} \overset{e}{\rightarrow} c_{18})]$. 

**Looking for the second generalization** Now we unfold the generalized term as follows: $T_7 = \{ [\tau]_{e}, ([\tau]_{e} \overset{e}{\rightarrow} a_1), ([\tau]_{e} \overset{e}{\rightarrow} a_2), (a_3 \overset{e}{\rightarrow} b_4), (a_3 \overset{e}{\rightarrow} b_5), (b_4 \overset{e}{\rightarrow} c_{12}), (b_5 \overset{e}{\rightarrow} c_{13}), (c_{13} \overset{e}{\rightarrow} d_{14}) \}$. $\tau \not\subseteq g_{b_3} \text{ and } t_{a_2} \not\subseteq g_{b_3} \text{ forbid to generalize } g_{b_3} \text{ and cause unfolding of } t_{c_{13}}$. We have $T_8 = \{ \ldots (a_3 \overset{e}{\rightarrow} b_5), (a_3 \overset{e}{\rightarrow} b_4), (b_5 \overset{e}{\rightarrow} c_{12}), (b_4 \overset{e}{\rightarrow} c_{13}), (c_{13} \overset{e}{\rightarrow} d_{14}) (c_{14} \overset{e}{\rightarrow} d_{15}), (c_{15} \overset{e}{\rightarrow} d_{16}) \}$. Here the new vertices were generated from the cases $\text{rm}$, $\text{wh3A}$, $\text{wm}$. For any ancestor $[n]_{e}$ of the open vertex $c_{13}$ we have $\eta \not\subseteq t_{c_{13}}$. UNFOLD rule yields: $T_9 = \{ \ldots (b \overset{e}{\rightarrow} c_{13}), (c_{13} \overset{e}{\rightarrow} d_{14}), (c_{14} \overset{e}{\rightarrow} d_{15}), (c_{15} \overset{e}{\rightarrow} d_{16}) \}$. $c_{17} = [\langle \text{inv e.x)(mod)(sh I e.z)(exc)(own)>\text{ in } <L (\text{time e.t) e.h}>]^a$, $(d_{14} \overset{e}{\rightarrow} c_{17})]$. $c_{18} = [\langle \text{Let e.h eq <<R s.m (inv e.x)(mod)(sh I e.z)(exc)(own)>> in <L (\text{time e.t) e.h}>]^a$, $(d_{14} \overset{e}{\rightarrow} c_{18})]$. 

Hence, when we will finish the proof this more general statement (with respect to the safety of the protocol MOESI) will be proved.
Now we close the open vertex \( d_{14}^1 \) with its ancestor \( b_5 \) and consider its unready sibling \( d_{15}^1 \). We unfold \( t_{d_{15}} \): 

\[
T_{10} = \{ \ldots (c_{13} \rightarrow d_{14}^1), (c_{13} \rightarrow d_{15}^1), (c_{13} \rightarrow d_{16}^1), (c_{13} \rightarrow d_{17}^1) \}. 
\]

\( e_{19} = [(\text{inv } e.z \text{ e.x})(\text{mod})(\text{sh})(\text{exc I})(\text{own})] \),

\( e_{20} = [\langle \text{let } e \cdot h \rangle \text{ eq } \langle R \text{ s.m } (\text{inv e.z e.x})(\text{mod})(\text{sh})(\text{exc I})(\text{own}) \rangle \}
\in \langle L \text{ (time e.t) e.h) } \rangle^a, 
\]

\( (d_{15}^1 \rightarrow e_{19}^1), (d_{16}^1 \rightarrow e_{19}^1) \). 

The relation \( \preceq \) forbids generalization of the term \( t_{d_{15}} \). We unfold \( t_{e_{20}} \):

\[
T_{11} = \{ \ldots , (d_{15}^1 \rightarrow e_{19}), (d_{15}^1 \rightarrow e_{19}^1), (e_{20} \rightarrow f_{21}^1), (e_{20} \rightarrow f_{22}^1), (e_{20} \rightarrow f_{22}^1), (e_{20} \rightarrow f_{23}^1) \}
\]

Here the new vertices were generated from the cases \( rm, wh2, \text{ and we have splitted the cases } rm, \text{ and we accordingly with SPLIT rule (the section } [\text{Restrictions on Term-rewriting Systems}] \) ). The term \( t_{e_{20}} \) cannot be generalized. We unfold \( t_{f_{21}^1} \): 

\[
T_{12} = \{ \ldots , (b_6 \rightarrow c_{12}), (b_6 \rightarrow c_{13}), (c_1 \rightarrow d_{14}^1), (c_1 \rightarrow d_{15}^1), (c_1 \rightarrow d_{16}^1), (d_{15}^1 \rightarrow e_{19}^1), 
\]

\[
(d_{21}^1 \rightarrow e_{20}^1), (e_{20} \rightarrow f_{21}^1), (e_{20} \rightarrow f_{22}^1), (e_{20} \rightarrow f_{23}^1), (e_{20} \rightarrow f_{23}^1) \}
\]

\( \bar{h}_{24} = [(\text{inv e.z e.x})(\text{mod})(\text{sh I I})(\text{exc})(\text{own})] \), 

\( \bar{h}_{25} = [\langle \text{let } e.h \rangle \text{ eq } \langle R \text{ s.m } (\text{inv e.z e.x})(\text{mod})(\text{sh I I})(\text{exc})(\text{own}) \rangle \}
\in \langle L \text{ (time e.t) e.h) } \rangle^a, 
\]

\( (f_{21}^1 \rightarrow h_{24}^1), (f_{21}^1 \rightarrow h_{25}^1) \). 

Now we close the open vertex \( f_{21}^1 \) with its ancestor \( b_5 \). The term \( f_{21}^2 \) is unfolded and closed likewise the \( f_{21}^1 \). We skip this case \( (T_{13}) \) and afterwards we have:

\[
T_{14} = \{ \ldots , (b_7 \rightarrow c_{14}), (c_{14} \rightarrow d_{14}^1), (c_{14} \rightarrow d_{15}^1), (d_{15}^1 \rightarrow e_{19}^1), 
\]

\[
(e_{20} \rightarrow f_{21}^1), (e_{20} \rightarrow f_{22}^1), (e_{20} \rightarrow f_{23}^1), (e_{20} \rightarrow f_{23}^1) \}
\]

UNFOLD rule applied to \( f_{22}^1 \) yields:

\[
T_{15} = \{ \ldots , (e_{20} \rightarrow f_{21}^1), (e_{20} \rightarrow f_{22}^1), (e_{20} \rightarrow f_{23}^1), (e_{20} \rightarrow f_{23}^1) \}
\]

\( \bar{h}_{26} = [(\text{inv e.z e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own})] \), 

\( \bar{h}_{27} = [\langle \text{let } e.h \rangle \text{ eq } \langle R \text{ s.m } (\text{inv e.z e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \}
\in \langle L \text{ (time e.t) e.h) } \rangle^a, 
\]

\( (f_{22}^1 \rightarrow h_{26}^1), (f_{22}^1 \rightarrow h_{27}^1) \). 

The relation \( \preceq \) forbids generalization of the term \( t_{f_{22}} \). We unfold \( t_{h_{27}} \):

\[
T_{16} = \{ \ldots , (e_{20} \rightarrow f_{21}^1), (e_{20} \rightarrow f_{22}^1), (f_{22} \rightarrow h_{26}^1), (f_{22} \rightarrow h_{27}^1), 
\]

\( (h_{26}^1 \rightarrow i_{28}^1), (h_{27}^1 \rightarrow i_{28}^1), (h_{27}^1 \rightarrow i_{28}^1), (h_{27}^1 \rightarrow i_{28}^1) \}. 
\]

Here the new vertices were generated from the cases \( rm, \text{ and we have splitted these cases accordingly with SPLIT rule. The term } h_{27} \text{ cannot be generalized. We unfold } t_{i_{28}^1} : 

\[
T_{17} = \{ \ldots , (f_{22}^1 \rightarrow h_{27}^1), (f_{22}^1 \rightarrow h_{27}^1), (f_{22}^1 \rightarrow h_{27}^1), (f_{22}^1 \rightarrow h_{27}^1) \}
\]

\( j_{30} = [(\text{inv e.z e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own})] \), 

\( j_{31} = [\langle \text{let } e.h \rangle \text{ eq } \langle R \text{ s.m } (\text{inv e.z e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \}
\in \langle L \text{ (time e.t) e.h) } \rangle^a, 
\]

\( (i_{28} \rightarrow j_{30}^1), (i_{28} \rightarrow j_{30}^1) \). 

The relation \( \preceq \) forbids generalization of the term \( t_{i_{28}^1} \). We unfold \( t_{j_{31}} : 

\[
T_{18} = \{ \ldots , (h_{27} \rightarrow i_{28}^1), (h_{27} \rightarrow i_{28}^1), (h_{27} \rightarrow i_{28}^1), (i_{28} \rightarrow j_{30}^1), 
\]

\( (i_{28} \rightarrow j_{31}^1), (j_{31} \rightarrow k_{28}^1), (j_{31} \rightarrow k_{28}^1), (j_{31} \rightarrow k_{28}^1), (j_{31} \rightarrow k_{28}^1), (j_{31} \rightarrow k_{28}^1) \). 
\]

Here the new vertices were generated from the cases \( rm, \text{ and we and we splitted the cases } rm, \text{ and we and we splitted the cases } rm, \text{ and we and } \text{ and we splitted the cases } rm, \text{ and we and we splitted the cases } rm, \text{ and we. The term } j_{31} \text{ cannot be generalized.} \)
We unfold \( t_{k_{32}} \): \( T_{10} = \{ \ldots (h_{27} \xrightarrow{e} i_{281}), (h_{27} \xrightarrow{e} i_{282}), (h_{27} \xrightarrow{e} i_{283}), (i_{281} \xrightarrow{e} j_{30}), (i_{281} \xrightarrow{e} j_{31}), (j_{31} \xrightarrow{e} k_{32}), (j_{31} \xrightarrow{e} k_{32}), (j_{31} \xrightarrow{e} k_{32}), (j_{31} \xrightarrow{e} k_{32}) \} \).

Now there exists the vertex \( i_{281} \), an ancestor of this vertex \( k_{32} \), and \( t_{i_{281}} \leq t_{k_{32}} \) holds. GENERALIZE rule constructs the term
\[
g_{i_{281}} = \langle L \langle \text{time e.t} \rangle \langle \text{e.h} \rangle \rangle \langle \text{mod} \langle \text{sh I e.z} \rangle \langle \text{exc} \rangle \langle \text{own I} \rangle \rangle.
\]

The term \( g_{i_{281}} \) generalizes both \( t_{i_{281}} \) and \( t_{k_{32}} \). The next tree to be developed is:
\[
T_{20} = \{ \ldots (j_{20} \xrightarrow{e} i_{281}), (j_{20} \xrightarrow{e} h_{27}), (j_{20} \xrightarrow{e} u_{281}), (j_{20} \xrightarrow{e} i_{282}), (j_{20} \xrightarrow{e} i_{283}), \}
\]

Note that we have replaced the term labelling the vertex \( i_{281} \). That is the second hypothesis generated by generalization. In fact the hypothesis is the last; henceforth we shall finish the proof without using of the GENERALIZE rule. The both hypotheses generated by generalization will be proved.

**Proof without generalization** Now we unfold the generalized term as follows:
\[
T_{21} = \{ \ldots (j_{21} \xrightarrow{e} h_{27}), (j_{21} \xrightarrow{e} i_{281}), (j_{21} \xrightarrow{e} i_{282}), (j_{21} \xrightarrow{e} i_{283}), \}
\]

The relation \( \leq \) forbids generalization of the term \( g_{i_{281}} \). We unfold \( t_{j_{30}} \):

\[
T_{22} = \{ \ldots (h_{27} \xrightarrow{e} i_{281}), (h_{27} \xrightarrow{e} i_{282}), (h_{27} \xrightarrow{e} i_{283}), \}
\]

Here the new vertices were generated from the cases \( r_{m}, w_{h34}, w_{h38}, w_{m} \). The term \( t_{j_{30}} \) cannot be generalized. We unfold \( t_{k_{42}} \):

\[
T_{23} = \{ \ldots (i_{281} \xrightarrow{e} j_{30}), (i_{281} \xrightarrow{e} k_{42}), (i_{281} \xrightarrow{e} k_{42}), (i_{281} \xrightarrow{e} k_{42}), \}
\]

Here we close the open vertex \( k_{40} \) with \( i_{281} \) and unfold its sibling \( t_{k_{41}} \):

\[
T_{24} = \{ \ldots (i_{281} \xrightarrow{e} j_{30}), (j_{30} \xrightarrow{e} k_{41}), (j_{30} \xrightarrow{e} k_{41}), (j_{30} \xrightarrow{e} k_{41}), \}
\]

We omit the development of \( t_{k_{42}} (T_{25}) \) and consider its sibling \( k_{43} \). \( t_{k_{43}} \leq t_{k_{42}} \) implies the vertex \( k_{43} \) can be unfolded and closed likewise \( k_{42} \). We omit its development
We see the next vertex to be unfolded is the second child of $h_2^7$. We denote the completely closed part of the tree as $T$, and unfold the term $t_{i_{292}}:

\begin{align*}
T_{28} &= \{ \ldots (f_{22} \leftarrow h_{27}), (h_{27} \leftarrow i_{28}), (h_{27} \leftarrow i_{29}), (h_{27} \leftarrow i_{30}), (h_{27} \leftarrow i_{31}) \}, \\
T_{29} &= \{ \ldots (c_{13} \leftarrow d_{13}), (c_{13} \leftarrow d_{16}), (d_{15} \leftarrow e_{10}), (d_{15} \leftarrow e_{30}), (e_{20} \leftarrow f_{21}), (e_{20} \leftarrow f_{22}), (e_{20} \leftarrow f_{23}), (f_{22} \leftarrow h_{28}), (f_{22} \leftarrow h_{27}), \\
& \quad (h_{27} \leftarrow i_{28}), (h_{27} \leftarrow i_{29}), (h_{27} \leftarrow i_{30}), (h_{27} \leftarrow i_{31}), T_c, \\
T_{30} &= \{ \ldots (c_{13} \leftarrow d_{13}), (c_{13} \leftarrow d_{14}), (e_{13} \leftarrow d_{14}), (c_{13} \leftarrow d_{15}), (c_{13} \leftarrow d_{16}), T_{c1} \}. \\
\end{align*}

The next term to be unfolded is $t_{i_{292}}: T_{33} = \{ \ldots (d_{16} \leftarrow c_{13}), (c_{13} \leftarrow d_{14}), (c_{13} \leftarrow d_{15}), (c_{13} \leftarrow d_{16}), (c_{13} \leftarrow d_{13}), T_{c1} \}, e_{53} = [\text{inv e.e.x}(\text{mod})(\text{sh})(\text{exc I})(\text{own I})]^c, \\
\begin{align*}
e_{53} &= [\text{Let e.h eq } & \text{R s.m (inv e.e.x)(mod)(sh)(exc I)(own I)}] \\
& \quad \text{in } \langle \text{L (time e.t) e.h} \rangle \rangle^u, \\
(d_{16} \leftarrow c_{13}), (c_{13} \leftarrow d_{14}), (c_{13} \leftarrow d_{15}), (c_{13} \leftarrow d_{16}) \}. \\
\end{align*}
We close the open vertex $b_4^*$ with $d_1^5$:

\[ T_{35} = \{ [\tau]^c, ([\tau]^c \xrightarrow{\iota} a_1^5), ([\tau]^c \xrightarrow{\iota} a_2^5), (a_2^5 \xrightarrow{\iota} b_5^5), (b_5^5 \xrightarrow{\iota} c_{13}^5), (c_{13}^5 \xrightarrow{\iota} d_4^5), (c_{13}^5 \xrightarrow{\iota} d_{15}), (c_{13}^5 \xrightarrow{\iota} d_{16}), T_1 \}. \]

The tree $T_{35}$ is completely closed. The inductive proof has been finished. □

See the figure 1 for the oriented graph of this proof.

**Fig. 1.** Graph of the automatic proof.

### References

\[ \tau = \langle L \ (\text{time e.time})(\text{inv I e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{b_3} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ g_{b_3} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{b_4} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{b_7} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{b_8} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{b_9} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{b_{14}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{b_{15}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{b_{16}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{f_{211}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{f_{212}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{f_{22}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{f_{231}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{f_{232}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{f_{281}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{f_{282}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{f_{291}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{f_{292}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{k_{321}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{k_{322}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{k_{33}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{k_{34}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{k_{341}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{k_{342}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{k_{40}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{k_{41}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{k_{42}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{k_{43}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{k_{431}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{k_{432}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{k_{44}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{k_{441}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{k_{442}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

\[ t_{k_{443}} = \langle L \ (\text{time e.t})(\text{inv e.x})(\text{mod})(\text{sh})(\text{exc})(\text{own}) \rangle \]

Table 1. MOESI configurations.
24. Lisitsa, A.P., Nemytykh, A.P.: A Note on Specialization of Interpreters. Accepted by the 2nd International Computer Science Symposium in Russia - CSR07.