Reachability Analysis in Verification via Supercompilation

Alexei Lisitsa[1] and Andrei P. Nemytykh[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. We present an approach to verification of parameterized systems, which is based on program transformation technique known as supercompilation. In this approach the statements about safety properties of a system to be verified are translated into the statements about properties of the program that simulates and tests the system. The supercompilation is used then to establish the required properties of the program. In this paper we show that reachability analysis performed by supercompilation can be seen as the proof of a correctness condition by induction. We formulate suitable induction principles and proof strategies and illustrate their use by examples of verification of parameterized protocols.

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

1 Introduction

The verification of infinite-state or parameterized problems is, in general, an undecidable problem. The research in this area is focused on finding restricted classes of problems, for which verification is decidable and the development of efficient verification procedures for practical applications. The research is active and taking different routes [10, 8, 3, 2, 1]. But still many practically interesting verification problems lie outside the scope of existing automated verification methods and further development of these methods is required.

One of the recent interesting and promising directions for tackling infinite-state, or parameterized, verification is to apply the methods developed in the area of *program transformation* and *metaprogramming*, and in particular, *program specialization* [11, 19, 18].

In this paper we are interested in one particular approach in program transformation and specialization, known as supercompilation[3]. *Supercompilation* [35]

⋆ The second author is supported by the Program for Basic Research of the Presidium of Russian Academy of Sciences (as a part of "Development of the basis of scientific distributed informational-computing environment on the base of GRID technologies"), and the Russian Ministry of Sciences and Education (grant 2007-4-1.4-18-02-064).

[3] from *super*vised *compilation*

has not drawn much attention yet in the context of verification, although it has been mentioned in [19, 18] as potentially applicable here. The supercompilation is a powerful semantic based program transformation technique [35, 38, 33] having a long history well back to the 1960-70s, when it was proposed by V. Turchin. The main idea behind a supercompiler is to observe the behavior of a functional program P running on *partially* defined input with the aim to define a program, which would be equivalent to the original one (on the domain of latter), but having improved properties. The supercompiler unfolds a potentially infinite tree of all possible computations of a parameterized program. In the process, it reduces the redundancy that could be present in the original program. It folds the tree into a finite graph of states and transitions between possible (paramemetrized) configurations of the computing system. And, finally, it analyses global properties of the graph and specializes this graph with respect to these properties (without an additional unfolding). The resulting definition is constructed solely based on the meta-interpretation of the source program rather than by a (step-by-step) transformation of the program.

The result of supercompilation may be a specialized version of the original program, taking into account the properties of partially known arguments, or just a re-formulated, and sometimes more efficient, equivalent program (on the domain of the original) [14].

Turchin's ideas have been studied by a number of authors for a long time and have, to some extent, been brought to the algorithmic and implementation stage [28]. From the very beginning the development of supercompilation has been conducted mainly in the context of the Refal programming language [37, 27], another creation of V.Turchin. A number of the simplest model supercompilers for subsets of LISP-like languages were implemented as well with an aim to formalize some aspects of the supercompilation algorithms [32, 34, 33]. The most advanced supercompiler for Refal is SCP4 [28, 26, 25, 27].

In [21–24] we proposed to use supercompilation for verification of parameterized systems using a particular scheme of *parameterized testing*. Using this scheme we translate the statements about safety properties of a system to be verified into the statements about properties of the program that *simulates and tests* the system. The supercompilation is used then to establish the required properties of the program. We have conducted series of experiments on verification of parameterized *cache coherence protocols* and successfully verified [22] all cache coherence protocols presented in [5] and [7]. We have also verified in this way parameterized Java MetaLock algorithm and series of Petri Nets models. This work started mainly as an experiment driven one and the approach proved to be empirically successful. This left however the questions on its correctness and completeness for classes of verification problems open. In this paper we address the issue of correctness of proposed method. We develop a formal model, which renders supercompilation process in the particular context of parameterized testing as a reachability analysis for term-rewriting systems by means of inductive proofs of safety properties. This establises the correctness of the method.

Further we illustrate our method by verification of parameterized MOESI protocol [5]. Interestingly enough, using supercompilation to perform parameterized testing allows not only to verify the protocol but also to discover new facts about the protocol. The facts are formulated by automatic generalization of configurations - one of the tools of supercompilation. In particular, an analysis of the supercompilation trace shows that the protocol is correct with more general assumptions on the initial state than reported in [5].

The paper is organized as follows. In the next section we give general description of our *verification via parameterized testing* approach in language-independent terms. Section 3 presents the formal model and correctness result. Then in section 4 we introduce some of the strategies leading to successful verification of a class of parameterized cache coherence protocols. In section 5 we present a free monoid of terms and specify the strategies of the supercompiler SCP4 in its terms. Detailed verification of the MOESI protocol using these strategies is presented in the Appendix.

2 Parameterized Testing

In this section we describe our general technique for the verification of parameterized systems. The technique is based on the translation of the statements about *safety* properties of a system to be verified into the statements about properties of the program that *simulates and tests* the system.

The scheme works as follows. Let S be a parameterized system (a protocol) and we would like to establish some safety property P of S. We write a program φ_S simulating execution of S for n steps, where n is an input parameter. Let the n be given in the unary system, as a string of characters. If the system is nondeterministic, we label each step with an action, whose value is assumed to be chosen at the branching point of execution, e.g. it may be a character labelling the choice. Thus, we assume that given the values of input parameter n, the program φ_S returns the state of the system S after the execution of n steps of the system, following the choices provided by the labels of the steps. Let $T_P(\_)$ be a testing program, which given a state s of S returns the result of testing the property P on s (*True* or *False*). Consider a composition $T_P \circ \varphi_S$. This program first simulates the execution of the system and then tests the property required. Let the both programs terminate. Now the statement "the safety property P holds in any possible state reachable by the execution of the system S from an initial state" is equivalent to the statement "the program $T_P(\varphi(n))$ never returns the value *False*, no matter what values are given to the input parameter".

In practical implementation of the scheme we use functional programming language Refal to implement a program $T_P(\varphi_S(n))$ and optimizer SCP4 (a supercompiler) to transform the program to a form, from which one can easily establish the required property.

The idea of using testing and supercompilation for the verification purposes is not new. In the classical paper [35] V.Turchin writes: *Proving the correctness of a program is theorem proving, so a supercompiler can be relevant. For example,*

if we want to check that the output of a function $F(x)$ always has the property $P(x)$, we can try to transform the function $P(F(x))$ into an identical T. The idea has not been tried until recently for the problems interesting for verification community. Our experiments have shown that indeed, the idea is viable and can be adopted for non-trivial verifications problems for parameterized distributed systems.

3 Correctness Issue and Formal Model

One of the immediate questions posed by almost everyone seeing the approach in work for the first time is "Is this correct at all? Why should I believe your claims about verification?"

Firstly, one can argue as follows. It has been shown, in particular in [32, 34, 31] that (variants of) supercompilation is a correct transformation, in a sense it always returns (if any) the program equivalent to the input program (on the domain of latter). Then we repeat the argument from Section 2. We should note, in this respect, that SCP4 [26, 25, 28] is a large program dealing with the concrete functional language Refal, which has specific semantic assumptions, like built-in associativity of concatenation as a term forming construct. Furthermore, SCP4 supercompiler, is a result for the more than two decades development and it is highly optimized program, implementing different strategies which can be tailored by the user to the particular cases. Proving the correctness of the whole SCP4 is far from being trivial and is, actually, irrelevant to our experiments. Even if we accept the correctness, it does not explain *why* supercompilation works for establishing correctness properties. We address these issues in the present paper by developing a formal model, which renders supercompilation process (in the case of verification tasks) as an inductive proof of safety properties. That establishes the correctness of the method. The formal model is a very simplified and refined theoretical version of SCP4, which, nevertheless, is sufficient for verification of a class of (parameterized) cache coherence protocols.

In this paper we confine ourselves by the claim that supercompiler SCP4 indeed implements the formal model we present. We provide some relevant comments but detailed discussion of the claim lies outside the scope of this paper. The model formulated in terms of term rewriting systems.

3.1 Term Rewriting Systems and Safety Properties

Let $\mathcal{V}$ be a denumerable set of symbols for variables and $\mathcal{F} = \cup_i \mathcal{F}_i$ be a finite set of functional symbols, here $\mathcal{F}_i$ is a set of functional symbols of arity i. Let $\mathcal{T}(\mathcal{V}, \mathcal{F})$ be a free algebra of all terms build with variables from $\mathcal{V}$ and functional symbols from $\mathcal{F}$ in a usual way. Let every $\mathcal{F}_i$ be divided into disjoint sets $\mathcal{F}_i = \mathcal{F}n_i \cup \mathcal{C}_i$. We refer to $\mathcal{F}n_i$ as function names and to $\mathcal{C}_i$ as constructor names. Let $\mathcal{C} = \cup_i \mathcal{C}_i$. A term without function names is passive. Let $\mathcal{G}(\mathcal{T}) \subset \mathcal{T}(\mathcal{V}, \mathcal{F})$ be the set of ground terms, i.e. terms without variables. Let $\mathcal{O}(\mathcal{T}) \subset \mathcal{G}(\mathcal{T})$ be the set of object

terms, i.e. ground passive terms. For a term t we denote the set of all variables in t by $V(t)$.

A substitution is a mapping $\theta : \mathcal{V} \to \mathcal{T}(\mathcal{V}, \mathcal{F})$. A substitution can be extended to act on all terms homomorphically. A substitution is called *ground*, *object*, or *strict* iff its range is a subset of $\mathcal{G}(\mathcal{T})$, $\mathcal{O}(\mathcal{T})$ or $\mathcal{T}(\mathcal{V}, \mathcal{C})$ (i.e. passive terms), respectively. We use notation $s = t\theta$ for $s = \theta(t)$, call s be an *instance* of t and denote this fact by $s \ll t$.

A term-rewriting system is a pair $P = \langle t, R \rangle$, where t is a term called *initial* and R is a finite set of rules of the form $f(p_1, \ldots, p_k) \to r$, where $f \in \mathcal{F}n_k$, $\forall i \ (p_i \in \mathcal{T}(\mathcal{V}, \mathcal{C}))$[4], $r \in \mathcal{T}(\mathcal{V}, \mathcal{F})$, $V(r) \subseteq V(f(p_1, \ldots, p_k))$.

Given a set of rules R define one-step transition relation $\Rightarrow_R \subseteq \mathcal{T}(\mathcal{V}, \mathcal{F}) \times \mathcal{T}(\mathcal{V}, \mathcal{F})$ as follows: $t_1 \Rightarrow_R t_2$ holds iff there exist a strict substitution θ and a rule $(l \to r) \in R$ such that $t_1 = l\theta$ and $t_2 = r\theta$. *Reachability* relation $\Rightarrow_R^*$ is a *transitive* and *reflexive* closure of $\Rightarrow_R$. Notice, that any term reachable for a ground term is also ground.

Definition 1. *A binary relation $\Rightarrow$ on a set $\mathcal{T}$ is terminating (or well-founded) if there exists no infinite chain $t_1 \Rightarrow t_2 \Rightarrow t_3 \Rightarrow \ldots$ of elements of $\mathcal{T}$.*

Henceforth we assume that *transitive* closure $\Rightarrow_R^+$ of the restriction of $\Rightarrow_R$ on $\mathcal{G}(\mathcal{T}) \times \mathcal{G}(\mathcal{T})$ is terminating.

An arbitrary subset Q of $\mathcal{O}(\mathcal{T})$ is called a *property*. Let q be a finite set (*collection*) of passive terms. A property Q_q defined by q is a set of all object instances of all terms from q, that is $Q_q = \{\tau \mid \tau \in \mathcal{O}(\mathcal{T}) \wedge \exists \rho \in q \ (\tau \ll \rho)\}$

We consider the following *reachability* problem on for term-rewriting systems.

Verification of safety property
Given: *A term-rewriting system $P = \langle t, R \rangle$ and property Q_q.*
Question: *Is it true that all passive terms reachable in P from any ground instance of t do not satisfy the property Q_q? In formal notation, is the statement*

$$\forall s \in \mathcal{O}(\mathcal{T})(\forall t' \in \mathcal{O}(\mathcal{T})((t' \ll t) \wedge (t' \Rightarrow_R^* s)) \to s \notin Q_q)$$

true?

Many interesting verification problems for parameterized systems may be reduced to the above problem. See the section 7 for an example. In the next subsection we present a method suitable for solving such a problem and demonstrate its correctness.

3.2 Inductive Proofs of Safety Properties

Consider an instance of the above verification problem $I = (\langle t, R \rangle, Q_q)$.

The proof of the safety property for I can be established by constructing successful *proof attempt* which consists of a sequence of trees. Vertices of trees will be labeled by terms. For a vertex a denote by t_a the term labeling a.

[4] For simplicity we use only such kind of term-rewriting systems.

We assume that we have a testing procedure, which given a vertex a checks whether *all ground instances* of the t_a *do not satisfy* the property Q_q.

Another assumption is that any vertex in a tree is labelled as *unready*, *open* or *closed* (one flag per vertex) and all generated vertices are unready until they are explicitly open. We assume also that when any vertex of the proof tree labeled by a passive term is generated it is immediately tested. If the testing produces the negative result the whole proof tree building procedure stops and returns the answer NO to the verification problem, otherwise the vertex is closed.

Given a directed tree T and its edge $(a \stackrel{e}{\rightarrow} b)$, we say the vertex a is the *parent* of b and b is a *child* of a. A vertex a_1 is an ancestor of a vertex a_n if there exists a sequence of edges of T such that $(a_1 \stackrel{e}{\rightarrow} a_2), (a_2 \stackrel{e}{\rightarrow} a_3), \ldots, (a_{n-1} \stackrel{e}{\rightarrow} a_n)$.

Definition 2. *For a given* $I = (\langle t, R\rangle, Q_q)$ *a* proof attempt *is a sequence of directed trees* $T_0, T_1, \ldots$ *such that* T_0 *is generated by the START rule, and* T_{i+1} *is obtained from* T_i *by application of one of the following rules: UNFOLD, CLOSE, GENERALIZE.*

The proof rules are defined as follows

START Create a root of the tree, label it by the initial term t of the term rewriting system.

UNFOLD Choose any of the unready vertices a with the labeling term t_a and generate all terms $t_1, \ldots t_n$ such $t_a \Rightarrow_R t_i$. For every such t_i create a child vertex a_i for a and put $t_{a_i} = t_i$. Open the vertex a. If the parent of a is open, then close the parent.

CLOSE I Choose any of the open vertices a and check whether there is a closed vertex b, such that $t_a \ll t_b$. If yes close the vertex a and delete its children. If there are no such a b do nothing.

CLOSE II Choose any of the open vertices a and check whether all its children are closed there. If yes close the vertex a.

GENERALIZE Choose any of the open vertices a and any vertex b, ancestor of the a in the tree. Generate a term τ such that both $t_b \ll \tau$ and $t_a \ll \tau$ hold. Delete the subtree with the root b, except the vertex b itself. Replace the label t_b with τ. Mark the vertex b as unready.

Significance of the *unready* flag is related to effectiveness issue and will be considered in the section 4.

Definition 3. *A* proof *of an* I *is a finite proof attempt* $T_0, \ldots, T_n$ *for* I *such that all vertices in* T_n *are closed.*

Let R be a term rewriting system, $t \in \mathcal{T}(\mathcal{V}, \mathcal{F})$ and t_0 be a ground instance of the term t. Let $\bar{t_0} = t_0 \Rightarrow_R t_1 \Rightarrow_R t_2 \ldots \Rightarrow_R t_l$ be an arbitrary sequence of terms derived from t_0 by application of rules from R. Denote by $\mathcal{R}(t)$ the set of all passive terms reachable in R from any ground instance of t and $\mathcal{CR}(t)$ the set of all the sequences $\bar{g_0}$ such that g_0 is a ground instance of t and $g_{|\bar{g_0}|-1} \in \mathcal{R}(t)$. The following proposition is trivial.

Proposition 1. *Let t be a term and τ be a term such that $t \ll \tau$, then $\mathcal{CR}(t) \subset \mathcal{CR}(\tau)$ holds. (And hence $\mathcal{R}(t) \subset \mathcal{R}(\tau)$.)*

Theorem 1. *For an instance $I = (\langle t, R\rangle, Q_q)$ of the verification problem above if there is a proof for I then the answer for this I is YES.*

Proof Let $T_0, \ldots, T_N$ be a proof for I.

The statement of the theorem follows from the following statement. Let t_0 be a ground instance of the initial term t. Let $\bar{t} = t_0 \Rightarrow_R t_1 \Rightarrow_R t_2 \ldots \Rightarrow_R t_{l-1}$ be an arbitrary sequence of terms derived from t_0 by application of rules from R. Then every t_i is an instance of a term t_{a_i} for some vertex a_i of T. The proof of the statement is by induction on the length of the sequence. Let $|\bar{t}| = 1$, that is $\bar{t} = t_0$ By construction of the proof attempt $T_0, \ldots, T_N$ the label τ of the initial vertex of T_N is (possibly generalized several times) term t, i.e. we have $t \ll \tau$ and therefore $t_0 \ll \tau$. Notice that once a term labelling some vertex is generated it may be generalized several times later in the proof attempt by application of GENERALIZE rule.

Consider now the step of induction. Assume the statement for all sequences of the length up to some l and let $\bar{t} = t_0 \Rightarrow_R t_1 \Rightarrow_R t_2 \ldots \Rightarrow_R t_l$. By induction hypothesis we have $t_{l-1} \ll t_a$ for some vertex $a \in T_N$. Then two cases are possible.

If there are some children $a_1, \ldots, a_k$ of a in T_N then there exists some child a_j of a such that t_{a_j} is (possibly generalization of) the term t_l (by the semantics of UNFOLD rule). It follows then $t_l \ll t_{a_j}$.

If there are no children of a in T_N then t_a should be active, otherwise there could not be any term t_l such that $t_{l-1} \ll t_a$ and $t_{l-1} \Rightarrow_R t_l$. Moreover in that case the vertex a is closed by the application CLOSE I rule and there should be another vertex $b \in T_N$ such that $t_a \ll t_b$. If b has some children we repeat the argument for the previous case taking vertex b instead of a. If it does not we find yet another vertex c such that $t_a \ll t_b \ll t_c$ and repeat the argument for c. Notice that there is no more than finitely many vertices in T_N, so after finitely many steps this case is reduced to the previous one. Step of induction is proved.

It follows that any ground passive term derivable from t_0 is an instance of one of the passive terms in T_N. Since all reachable passive vertices in T_N are tested the statement of the theorem follows. □

Example 1. Let $f \in \mathcal{F}n_2$, $A, B \in \mathcal{C}_1$, $x, y, x_i, y_i \in \mathcal{V}$. Consider $I = (\langle t, R\rangle, Q_q)$. Here R is:

$f(B(x), y) = f(x, B(y))$;
$f(A(A(x)), y) = f(A(x), B(y))$;
$f(A(B(x)), y) = y$;

q contains the only term $A(x)$ and $t = f(B(x_1), y_1)$.

Let $[\tau]$ be a vertex labelled with a term τ. We denote each closed vertex as $[\tau]^c$, each open vertex as $[\tau]^o$ and each unready vertex as $[\tau]^u$. The first proof attempt is successful: START rule gives the tree T_0 containing the only vertex $a^u =$

$[f(B(x_1), y_1)]^u$, UNFOLD rule yields $T_1 = \{a^o, b^u = [f(x_2, B(y_1))]^u, (a^o \xrightarrow{e} b^u)\}$; after the second UNFOLD we have $T_2 = \{a^c, b^o, d_1^u = [f(x_3, B(B(y_1)))]^u, d_2^u = [f(A(x_4), B(B(y_1)))]^u, d_3^u = [B(y_1)]^c, (a^c \xrightarrow{e} b^o), (b^o \xrightarrow{e} d_1^u), (b^o \xrightarrow{e} d_2^u), (b^o \xrightarrow{e} d_3^u)\}$; now two applications of UNFOLD rule open d_1^u, d_2^u and close b^o; two applications of CLOSE rule close d_1^o and d_2^o with b^c as the witness. We have $T_6 = \{a^c, b^c, d_1^c, d_2^c, d_3^c, (a^c \xrightarrow{e} b^c), (b^c \xrightarrow{e} d_1^c), (b^c \xrightarrow{e} d_2^c), (b^c \xrightarrow{e} d_3^c)\}$, where all vertices are closed.

The second proof attempt fails: T_0, T_1, T_2 are the same as in the first attempt; GENERALIZE gives $T_3 = \{g^u = [f(x_3, y_3)]^u\}$. Now it is easy to see this attempt does not terminate.

The third proof attempt fails: T_0, T_1, T_2 are the same as in the first attempt; GENERALIZE gives $T_3 = \{g^u = [x_3]^u\}$. Now g^u can never be closed.

We show now that, in fact, the proof sequence is a compact representation of the inductive proof of the correctness condition (none of the ground instances of the reachable passive terms has the property Q_q). First, we formulate the induction scheme in general terms.

Let $\triangleright$ be a well-founded partial ordering on a set $\mathcal{K}$. Let $\mathcal{M}$ is the set of all minimal elements of $\mathcal{K}$: $\mathcal{M} = \{t \in \mathcal{K} \mid \neg\exists(\tau \in \mathcal{K}).(\tau \neq t) \wedge (t \triangleright \tau)\}$. Note that $\mathcal{M}$ is not empty. Let Q be a predicate on $\mathcal{K}$ and $\mathcal{S}$ be a subset of $\mathcal{K}$. The following induction scheme can be used then to prove that Q holds everywhere on $\mathcal{K}$ (we assume $y \triangleleft x \equiv x \triangleright y$ here):

$$\frac{(\forall t \in \mathcal{M}.Q(t)) \wedge (\forall x \in \mathcal{K}.(\forall y \in \mathcal{S}.y \triangleleft x \rightarrow Q(y)) \rightarrow Q(x))}{\forall x \in \mathcal{K}.Q(x)}$$

Retuning to our context, let $\mathcal{L}$ is the set of the terms generated by applications of GENERALIZE rule during the proof given above and t is the initial term of the I. Let H_g be the following hypothesis: "none of the ground instances of $g \in \mathcal{L}$ reaches a passive term having the property Q_q".

Then the proof given by the successful proof attempt can be considered as simultaneous proofs of all hypotheses H_g, such that each of them follows the inductive scheme given above and moreover the proofs may refer one to another. Here $\mathcal{K} = \mathcal{O}(\mathcal{T})$, $\triangleright$ is $\Rightarrow_R^+$, $Q(t) = H_t$, $\mathcal{M}_g$ is the set of all passive object terms reachable from all ground instances of g, and $\mathcal{S}_g$ is the set of the ground instances of the terms closed during applications of CLOSE rule. The subscript g indicates the concrete proof of H_g.

4 Towards Effectiveness

The proof procedure presented in the previous section is non-determinstic. That leads to necessity of development of deterministic proof strategies which would be complete and/or efficient for classes of verification problems. In this section we make first steps towards resolving these largely open issues, and present the strategies which empirically has turned out to be sufficient for (practically efficient) proofs of correctness of cache coherence protocols [5].

The second proof attempt given in the Example 1 demonstrates that critical information may be lost during an application of GENERALIZE rule. The information guaranteed transformation of the initial term uniformly on the values of the parameters. The start vertex is not a branching point: there exists the only edge outgoing from the vertex. Terminating of $\Rightarrow_R^+$ (see the section 3.1) means there cannot be an infinite sequence of such kind of vertices one after another. Thus it is desirable to exclude such vertices from generalization.

Definition 4. *An open or closed vertex b is* pivot *in a tree T_j iff b has at least two outgoing edges.*

A closed vertex can be both basic and pivot. Henceforth we impose the following retsriction on the strategy of rule applications: *both CLOSE and GENERALIZE rules choose only pivot vertices.*

Given two terms t_1 and t_2 there can be a number of different generalizations, see example 1 for the illustration. Aiming to preserve as much as possible the structure of the terms, we impose the next restriction on GENERALIZATION rule: *result of generalization of any two terms t_1 and t_2 should be most specific term τ*, meaning both $t_1 \ll \tau$ and $t_2 \ll \tau$ hold and for any other term ξ such that $(t_1 \ll \xi) \wedge (t_2 \ll \xi \ll \tau)$ implies that ξ equals to τ modulo variable's names.

Further restriction is concerned with the choice of terms to be generalized. In order to preserve the structure of terms it is natural and desirable to generalize only terms, which are similar (in a sense) one to another. There is delicate trade-off here. Informally, the fewer applications of GENERALIZE rule happened during a proof attempt the less information on the terms structure is lost and more chances to close the passive vertices. On the other hand, to close active vertices one may need more applications of GENERALIZE rule. The following criteria based on well-quasi-ordering have turned out to be empirically successful.

A *quasi-ordering* is any reflexive and transitive binary relation.

Definition 5. *A quasi-ordering $\preceq$ on a set T is a* well-quasi-ordering *if every infinite sequence $t_1, t_2, \ldots$ of elements of T contains t_i, t_j $(i < j)$ such that $t_i \preceq t_j$.*

Given a well-quasi-ordering $\preceq$ on $\mathcal{T}(\mathcal{V}, \mathcal{F})$, we specify the strategy choosing the vertices by GENERALIZE rule as follows: *choose any of the pivot open vertices a and any pivot vertex b, ancestor of the a in the tree such that $t_b \preceq t_a$; if there exists no such a b do nothing.*

Further, there can be a number of such vertices b. Intuitively, the closer a vertex b to the vertex a (among the all its ancestors) the closer any ground instance of the b to a passive ground term terminating evaluation of the instance by the term-rewriting system. So we add to the above generalization strategy the requirement *to choose the closest such a vertex b.*

All our experiments verifying the class parameterized protocols [5] were successful both under lazy (call by need) and under applicative (call by value) strategies developing the stack of functions. For simplicity we selected the applicative

strategy to demonstrate the main example given in the section 7. We encode this semantic concept in syntax as follows. Given a composition $t = f(\ldots, g(\ldots), \ldots)$, where $f, g \in \mathcal{F}n$, we transform the term to

$$\texttt{Let}(x,\ \texttt{eq},\ g(\ldots),\ \texttt{in},\ f(\ldots,\ x,\ \ldots)),$$

$\texttt{Let} \in \mathcal{F}n$ is a auxiliary name. The term $g(\ldots)$ is transformed recursively in the same fashion. We note the semantics of both the t and the transformed term is the same. We stress that without such representation of the composition the other strategies do not lead to successful experiments with the cache coherence protocols.

5 A Free Monoid of Terms

In this section we consider a free monoid of terms, which was actually used in our experiments. Using this data structure and concepts and strategies given above allows to obtain automatic proofs of correctness of cache coherence protocols from [5]. See also remarks in Section 6.

We construct the monoid from $\mathcal{T}(\mathcal{V}, \mathcal{F})$ by minor modification of definition. Let all the function names be unary $\mathcal{F}n_1$, while the constructor set be $\mathcal{C} = \mathcal{C}_2 \cup \mathcal{C}_1 \cup \mathcal{C}_0$. Let us denote terms constructed with a $f \in \mathcal{F}n_1$ as $\texttt{<}f\ \ t\texttt{>}$, where t is a term. Let $\mathcal{C}_2$ contains the only *associative* element named as concatenation, used in infix notation and denoted with the blank. The associativity allows to drop the parentheses of the constructor at all. Let $\mathcal{C}_1$ contains the only constructor, which denoted only with its parentheses (that is without a name). $\mathcal{C}_0 = \mathcal{K} \cup \{\lambda\}$. We denote the constants from $\mathcal{K}$ with its names: that is without the parentheses. The constant λ is denoted with nothing: it is the unit of the concatenation. Let the variable set $\mathcal{V}$ be disjoined in two sets $\mathcal{V} = \mathcal{E} \cup \mathcal{S}$, where the names from $\mathcal{E}$ are prefixed with 'e.', while the names from $\mathcal{S}$ – with 's.'. For a term t we denote the set all e-variables (s-variables) in t by $\mathcal{E}(t)$ (correspondingly $\mathcal{S}(t)$). $\mathcal{V}(t) = \mathcal{E}(t) \cup \mathcal{S}(t)$. The monoid of the terms may be defined with the following grammar:

$t\ \texttt{::=}\ \lambda\ \texttt{|}\ c\ \texttt{|}\ v\ \texttt{|}\ \texttt{<}f\ \ t\texttt{>}\ \texttt{|}\ t_1\ \ t_2\ \texttt{|}\ \texttt{(}t\texttt{)}$
$\lambda\ \texttt{::=}$

where $c \in \mathcal{K}$, $v \in \mathcal{V}, f \in \mathcal{F}n_1$. Thus a term is a finite sequence (including the empty sequence). We denote the constructed free monoid as $\mathcal{A}(\mathcal{V}, \mathcal{F})$. Any substitution has to map every $v \in \mathcal{S}$ into $\mathcal{K} \cup \mathcal{S}$.

5.1 Restrictions on Term-rewriting Systems

Given a term-rewriting system $\langle t, R\rangle$ on the set $\mathcal{A}(\mathcal{V}, \mathcal{F})$. Associativity of the concatenation simplifies the syntax structure of the terms, but it creates a problem with the one-step transition relation $\Rightarrow_R \subseteq \mathcal{A}(\mathcal{V}, \mathcal{F}) \times \mathcal{A}(\mathcal{V}, \mathcal{F})$, namely, given a term τ and a rule $(l \to r) \in R$, then there can be several substitutions matching τ with the l. Thus we have a new kind of non-determinism here. An example is as follows:

Example 2. $\tau = \texttt{<}f\ \ A\texttt{>}$ and $l = \texttt{<}f\ \ e.x\ \ e.y\texttt{>}$, where $A \in \mathcal{K}$, $e.x, e.y \in \mathcal{E} \subset \mathcal{V}$. There exist two substitutions matching the terms: the first is $\theta_1(e.x) = \lambda, \theta_1(e.y) = A$, the second is $\theta_2(e.x) = A, \theta_1(e.y) = \lambda$.

Multiplicity of $v \in \mathcal{V}$ in a term t is the number of occurrences of v in t. A variable $x \in \mathcal{E}(t)$ is closed in a term t iff (1) $t = (t_1)$ and x is closed in t_1; (2) $t = t_1 \dots t_n$, where there exists at most one $t_i = x$ and $\forall j$ the x is closed in t_j.

We impose the following restriction on the left sides of the rules from R. The multiplicity of any $v \in \mathcal{E}(l)$ equals 1 and v is closed in l. These restrictions exclude recursive equations that have to be solved when we are looking for the substitutions matching a given parameterized term with a left side of a rule. The following term $\tau = \texttt{<}f\ \ \texttt{(}A\ \ e.p\texttt{)}\ \ \texttt{(}e.p\ \ A\texttt{)>}$ and $l = \texttt{<}f\ \ \texttt{(}e.x\texttt{)}\ \ \texttt{(}e.x\texttt{)>}$ is an example showing that the recursive equation $A\ e.p = e.p\ A$ arises on $e.p$; the reason of the recursion is the fact that the multiplicity of $e.x \in \mathcal{E}(l)$ is 2.[5] The second example $\tau = \texttt{<}f\ \ e.p\texttt{>}$ and $l = \texttt{<}f\ \ e.x\ \ A\ \ e.y\texttt{>}$ as well as the example 2 demonstrate the problems, which are caused by unclosed variables (here both $e.x$ and $e.y$) in the left hand-sides of the rules.

Consider the example 2. Let us think of the τ as a left part of a rule ρ, while of the l as a term to be match with τ with the goal to unfold. The both substitutions given in the example 2 match the term l with τ. Hence, during the application of UNFOLD rule we have to take into account the both substitutions and generate two children of l from ρ. We solve this problem with the following additional sub-rule:

SPLIT Given a term t to be unfolded (with a rule $\rho = (l \to r)$) such that $\mathcal{E}(t)$ includes unclosed variables. Take a subterm of t of the form $\xi = t_1\ \dots\ e.x\ \dots\ e.y\ \dots t_n$ (i.e. the both variables $e.x, e.y \in \mathcal{E}(t)$ are not enclosed with the parenthesis) such that there exist at least two substitutions which match ξ with the corresponding subterm of l. Generate the following three substitutions $\theta_1(e.x) = s.n\ \ e.x_1, \theta_2(e.x) = \texttt{(}e.z\texttt{)}\ \ e.x_2, \theta_3(e.x) = \lambda$. Here $e.x_1, e.x_2, e.z$ are fresh variables from $\mathcal{E}$, $s.n$ is a fresh variable from $\mathcal{S}$. Unfold $t\theta_i$ with the rule ρ.

The SPLIT rule is recursive and terminates. See the section 7 for the examples using this rule.

The example 2 shows also another problem. The term l may be considered as a generalization of the term τ: $\tau \ll l$. The problems is: there exists a term $\xi = e.z$ such that $l \neq \xi, \tau \ll \xi$ and both $l \ll \xi$ and $\xi \ll l$ hold. Now we specify generalization. Given two terms $t_1, t_2 \in \mathcal{A}(\mathcal{V}, \mathcal{F})$ and the set G of all the most specific terms generalizing both t_1 and t_2 (see the section 4). Let $\nu_x(t)$ be the multiplicity of an $x \in \mathcal{E}(t)$. We use (as the result of generalization of t_1, t_2) $g \in G$ such that $\sum_{x \in \mathcal{E}(g)} \nu_x(g)$ is minimal over G.

[5] The solution of the equation is $e.p = A^*$.

5.2 The Well-quasi-ordering on $\mathcal{A}(\mathcal{V}, \mathcal{F})$

Given $t_1, t_2 \in \mathcal{A}(\mathcal{V}, \mathcal{F})$, there exist two elementary functions constructing a new term from the given term. The functions are $F_1(t_1, t_2) = t_1\ t_2$ and $F_2(t_1) =$ `(`t_1`)`. There exists also a family of functions $F_f(t_1) =$ `<`$f\ t_1$`>`, where $f \in \mathcal{F}n_1$. We consider a quasi-ordering such that: (1) with respect to it all these functions are monotone non-decreasing $t_1 \underline{\propto} F_1(t_1, t_2), t_1 \underline{\propto} F_2(t_1), t_1 \underline{\propto} F_f(t_1)$; (2) these functions are matched with the quasi-ordering: $t_1 \underline{\propto} t_2$ implies $F_2(t_1) \underline{\propto} F_2(t_2), F_f(t_1) \underline{\propto} F_f(t_2)$ and for any term t both $F_1(t, t_1) \underline{\propto} F_1(t, t_2)$ and $F_1(t_1, t) \underline{\propto} F_1(t_2, t)$ hold. The following relation is a variant of the Higman-Kruskal relation and is a well-quasi-ordering [12, 15].

Definition 6. *The homeomorphic embedding relation* $\underline{\propto}$ *is the smallest transitive relation on* $\mathcal{A}(\mathcal{V}, \mathcal{F})$ *satisfying the following properties, where* $h \in \mathcal{F}n_1, s, t, t_i \in \mathcal{A}(\mathcal{V}, \mathcal{F})$.

1. $\forall x, y \in \mathcal{E}.\ x \underline{\propto} y, \forall u, v \in \mathcal{S}.\ u \underline{\propto} v$;
2. $t \underline{\propto}$ `<`$h\ t$`>`$, t \underline{\propto}$ `(`t`)`$, t \underline{\propto} s\ t, t \underline{\propto} t\ s$;
3. $s \underline{\propto} t$, *then* `<`$h\ s$`>` $\underline{\propto}$ `<`$h\ t$`>`, `(`s`)` $\underline{\propto}$ `(`t`)`, $s\ t_1 \underline{\propto} t\ t_1, t_1\ s \underline{\propto} t_1\ t$.

Corollary 1. 1. $\lambda \underline{\propto} t \underline{\propto} t$, *where* λ *is the empty sequence;*
2. $\exists i_1, \ldots, i_j$ *such that* $1 \leq i_1 < i_2 < \ldots < i_j \leq n$, *then* $t_{i_1} \ldots t_{i_j} \underline{\propto} t_1 \ldots t_n$.

Given an infinite sequence of terms $t_1, \ldots, t_n, \ldots$, this relation is relevant to approximation of increasing loops in the sequence; or in other words to looking for the regular similar cases of mathematical induction on the structure of the terms. That is to say the cases, which allow refer one to another by a step of the induction. An additional restriction separates the basic cases of the induction from the regular ones. The restriction is:

$$\forall c \in \mathcal{K}.\texttt{()} \not\underline{\propto}\ \texttt{(}c\texttt{)} \wedge \forall v \in \mathcal{S}.\texttt{()} \not\underline{\propto}\ \texttt{(}v\texttt{)}.$$

We impose this restriction on the relation $\underline{\propto}$ and denote the obtained relation as $\preceq$. It is easy to see that such a restriction does not violate the quasi-ordering property. Note that the restriction may be varied in the obvious way, but for our experiments its simplest case given above is used to control applications of GENERALIZE rule and has turned out to be sufficient.

6 Discussion

In addition to the MOESI protocol described in the Appendix the supercompiler SCP4 verified by our scheme the following parameterized cache coherence protocols: IEEE Futerbus+, MESI, MSI, "The University of Illions", DEC Firefly, "Berkeley", Xerox PARC Dragon [5, 6]. All these protocols are specified analogously to the description given in the section 7. In the case of the MOESI protocol the time of automatic verification is 1 second (Windows XP/Service

Pack 2, Intel Pentium III, 450 MHz, 256 MB of RAM); verification of the other protocols takes times, which slightly differ from the indicated.

One of the questions left open is why do we work in terms of the free monoid $\mathcal{A}(\mathcal{V}, \mathcal{F})$ and how important is such a choice? Actually, supercompiler SCP4 is able to prove correctness of the main example considered in the section 7 encoded in terms of a free algebra terms too, but the proof is much more bulky as compared with the proof presented in section 7.3. Moreover, the proof in this case requires additional capabilities of the supercompiler which are not presented in our formal model. We leave detailed analsys and comparisons of different encodings to future work.

The work reported in this paper has started as mainly driven by experiments. There is still much work to be done, both theoretically and experimentally. On the theory side we would like to have the completeness results for classes of verification problems and particular strategies. The applicability of the strategies already implemented in SCP4 is also worth to explore further. Recent experiments have shown that SCP4 strategies are quite robust with respect to order in wich rewriting rules are encoded in Refal programs. For example, the above MOESI protocol can be verifed with any of 120 (=5!) permutations of rewriting rules for `RandomAction`. See [24] for details to this subject.

Finally, comparisons with related work, especially with [11, 19, 20] and [30] should be done. In both these approaches transformations of logic (as opposed to our functional) programs are used to perform verification of parameterized systems. Despite the differences in programing languages, systems encodings and verifications schemes used, all three approaches have a common ground and rely on variants of unfold/fold transformations.

References

1. Abdulla, P.A., Jonsson, B., Nilsson, M., Saksena, M.: A Survey of Regular Model Checking. In *Proc. 15th Int. Conf. on Concurrency Theory*, LNCS, 2004.
2. Baukus, K., Stahl, K., Bensalem, S., Lakhnech, Y.: Networks of Processes with Parameterized State Space. In *Electronic Notes in Theoretical Computer Science*, January 2004, vol. 50, no.4, pp 1–15.
3. Bjorner, N., Browne, A., Chang, E., Colon, M., Kapur, A., Manna, Z., Sipma, H.B., Uribe T.E.: STeP: Deductive-Algorithmic Verification of Reactive and Real-time Systems. In *Proc. International Conference on Computer Aided Verification, CAV'96*, vol. 1102 of LNCS, Springer-Verlag, pp.415-418, 1996
4. Clarke, E.M., Grumberg, Peled, D.: *Model Checking.* MIT Press, 1999
5. Delzanno, G.: Automatic Verification of Parameterized Cache Coherence Protocols. In *Proc. of the 12th Int. Conf. on Computer Aided Verification*, LNCS, vol. 1855, pp. 53-68 (2000)
6. Delzanno, G.: Automatic Verification of Cache Coherence Protocols via Infinite-state Constraint-based Model Checking, http://www.disi.unige.it/person/DelzannoG/protocol.html.
7. Delzanno, G.: Verification of Consistency Protocols via Infinite-state Symbolic Model Checking, A Case Study. In *Proc. of FORTE/PSTV*, 2000, pp: 171-188.

8. Delzanno, G.: Contsraint-based Verification of Paremeterized Cache Coherence Protocols. *Formal Methods in System Design* 23(3):257-301, 2003.
9. Ershov, A.P.: Mixed computation in the class of recursive program schema. *Acta Cybernetica*, 4(1), 1978.
10. Esparza, J.: Decidability of model checking of infinite state concurrent systems. *Acta Informatica*, 34:85-107, 1997.
11. Glück, R., Leuschel, M.: Abstraction-based partial deduction for solving inverse problems – a transformational approach to software verification. In *Proc. of Systems Informatics*, LNCS 1755, pages 93-100, Novosibirsk, Russia, 1999. Springer-Verlag.
12. Higman, G.: Ordering by divisibility in abstract algebras. Proc. London Math. Soc. **2(7)** (1952) 326–336
13. Jones, N.D., Gomard, C.K., Sestoft, P.: Partial Evaluation and Automatic Program Generation. (1993) Prentice Hall International
14. Korlyukov, A.V., Nemytykh, A.P.: Supercompilation of Double Interpretation. (How One Hour of the Machine's Time Can Be Turned to One Second), 2002. http://www.refal.net/~korlukov/scp2int/Karliukou_Nemytykh.pdf. Sources, demonstration: www.refal.net/~korlukov/demo_scp4xslt.zip.
15. Kruskal, J.B.: Well-quasi-ordering, the tree theorem, and vazsonyi's conjecture. Trans. Amer. Math. Society, **95** (1960) 210–225
16. Leuschel, M., Martens, B.: Global Control for Partial Deduction through Characteristic Atoms and Global Trees. *Proceeding of the PEPM'96*, LNCS 1110, Springer-Verlag, 1996.
17. Leuschel, M.: On the Power of Homeomorphic Embedding for Online Termination. In *Proc. of the SAS'98*, LNCS 1503, 1998.
18. Leuschel, M., Lehmann, H.: Program Specialization, Inductive Theorem Proving and Infinite State Model Checking, Invited talk,LOPSTR'03, Uppsala, 2003, avaialable at:www.ecs.soton.ac.uk/~mal/presentations/ITP_Lopstr03.ppt.
19. Leuschel, M., Lehmann, H.: Solving coverability problems of Petri nets by partial deduction. In *Proc. 2nd Int. ACM SIGPLAN Conf. on Principles and Practice of Declarative Programming (PPDP'2000)*, Montreal, Canada, pp: 268-279, 2000.
20. Leuschel, M., Massart, T.: Infinite state model checking by abstract interpretation and program specialisation. In A. Bossi, editor, *Logic-Based Program Synthesis and Transformation. In Proc. of LOPSTR'99*, LNCS 1817, pages 63-82, Venice, Italy, 2000.
21. Lisitsa, A.P., Nemytykh, A.P.: Towards Verification via Supercompilation. In *Proc. of COMPSAC 05, the 29th Annual International Computer Software and Applications Conference, Workshop Papers and Fast Abstracts*, pages 9-10, IEEE, 2005.
22. Lisitsa, A.P., Nemytykh, A.P.: Verification via Supercompilation. `http://www.csc.liv.ac.uk/~alexei/VeriSuper/`
23. Lisitsa, A.P., Nemytykh, A.P.: Verification as a Parameterized Testing (Experiments with the SCP4 Supercompiler). Programmirovanie. No.**1** (2007) (In Russian). English translation in J. Programming and Computer Software, Vol. **33**, No.1 (2007) 14–23, Pleiades Publishing, Ltd.
24. Lisitsa, A.P., Nemytykh, A.P.: A Note on Specialization of Interpreters. Accepted by the 2nd International Computer Science Symposium in Russia - CSR07.
25. Nemytykh, A.P.: A Note on Elimination of Simplest Recursions.. In Proc. of the ACM SIGPLAN Asian Symposium on Partial Evaluation and Semantics-Based Program Manipulation, (2002) 138–146, ACM Press

26. Nemytykh, A.P.: The Supercompiler SCP4: General Structure (extended abstract). In Proc. of the Perspectives of System Informatics, LNCS, **2890** (2003) 162–170, Springer-Verlag
27. Nemytykh, A.P.: Playing on REFAL. In: Proc. of the International Workshop on Program Understanding. A.P. Ershov Institute of Informatics Systems, Syberian Branch of Russian Academy of Sciences, pp:29-39, July 2003.
(ftp://www.botik.ru/pub/local/scp/refal5/nemytykh_PU03.ps.gz)
28. Nemytykh, A.P., Turchin, V.F.: The Supercompiler SCP4: sources, on-line demonstration, http://www.botik.ru/pub/local/scp/refal5/, (2000).
29. Romanenko, S.A.: Arity raiser and its use in program specialization. *Proceeding of the ESOP'90*, LNCS, 432:341–360, 1990.
30. Roychoudhury A., Ramakrishnan C.R.: Unfold/fold Transformations for Automated Verification of Parameterized Concurrent Systems. In *Program Development in Computational Logic*, LNCS 3049, 2004, pp 262-291, 2004
31. Sands, D.: Proving the correctness of recursion-based automatic program transformation. In *Theory and Practice of Software Development*, volume 915 of LNCS, pp 681–695, 1995.
32. Sørensen, M.H., Glück, R.: An algorithm of generalization in positive supercompilation. In *Logic Programming: Proceedings of the 1995 International Symposium*, pages 486–479. MIT Press, 1995.
33. Sørensen, M.H., Glück, R.: Introduction to Supercompilation. *Partial Evaluation - Practice and Theory*, DIKU 1998 International Summer School. June 1998.
http://repository.readscheme.org/ftp/papers/pe98-school/D-364.pdf
34. Sørensen, M.H., Glück, R., Jones, N.D.: A positive supercompiler. In *Journal of Functional Programming*, **6(6)** (1996) 811–838
35. Turchin, V.F.: The concept of a supercompiler. *ACM Transactions on Programming Languages and Systems*, 8:292–325, 1986.
36. Turchin, V.F.: The algorithm of generalization in the supercompiler. In *Proceedings of the IFIP TC2 Workshop, Partial Evaluation and Mixed Computation*, pages 531–549. Amsterdam: North-Holland Publishing Co., 1988.
37. Turchin, V.F.: Refal-5, Programming Guide and Reference Manual. Holyoke, Massachusetts. (1989) New England Publishing Co.
(electronic version: http://www.botik.ru/pub/local/scp/refal5/ ,2000)
38. Turchin, V.F.: Metacomputation: Metasystem transition plus supercompilation. *Proceeding of the PEPM'96*, LNCS, Springer-Verlag, 1110:481–509, 1996.
39. Turchin, V.F., Turchin, D.V., Konyshev, A.P., Nemytykh, A.P.: Refal-5: sources, executable modules. http://www.botik.ru/pub/local/scp/refal5/, (2000)
40. Wadler, P.: Deforestation: Transforming programs to eliminate tree. *Theoretical Computer Science*, 73:231–238, 1990.

7 Appendix. Example: MOESI protocol

In this section we apply the parameterized testing (described in Section 2) to the MOESI cache coherence protocol considered in [5]. We will work in terms of $\mathcal{A}(\mathcal{V}, \mathcal{F})$. G. Delzanno [5] describes evolution of this protocol as follows:

```
(rh) modified + owned + shared + exclusive ≥ 1 → .
(rm) invalid ≥ 1 →
       invalid' = invalid - 1, exclusive' = 0, modified' = 0,
```

```
       shared' = shared + exclusive + 1, owned' = owned + modified .
(wh1) modified ≥ 1 → .
(wh2) exclusive ≥ 1 →
       exclusive' = exclusive - 1, modified' = modified + 1 .
(wh3) shared + owned ≥ 1 → exclusive' = 1,
       shared' = 0, modified' = 0, owned' = 0,
       invalid' = invalid + exclusive + modified + owned + shared - 1.
(wm) invalid ≥ 1 → exclusive' = 1,
       shared' = 0, modified' = 0, owned' = 0,
       invalid' = invalid + exclusive + modified + owned + shared - 1 .
```

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

$$\texttt{invalid} = x + 1, \texttt{modified} = \texttt{shared} = \texttt{exclusive} = \texttt{owned} = 0.$$

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

```
-- (C1) exclusive + shared + owned ≥ 1, modified ≥ 1;
-- (C2) exclusive ≥ 1, shared + owned ≥ 1;
-- (C3) modified ≥ 2;
-- (C4) exclusive ≥ 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.

7.1 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 `time` and use the unary arithmetic: $0 = \lambda$, $n + 1 = \texttt{I}\ n$.

Let `time, inv, mod, sh, exc, own, rm, wh2, wh3A, wh3B, wm, I` $\in \mathcal{K}$ and `Loop`,
`RandomAction` $\in \mathcal{F}n_1$. Recall that `e.x`, ... $\in \mathcal{E}$ and `s.tm`, ... $\in \mathcal{S}$, where $\mathcal{E} \cup \mathcal{S} = \mathcal{V}$ (see the section 5). The rules of the MOESI protocol are encoded in term of $\mathcal{A}(\mathcal{V}, \mathcal{F})$ as follows:

```
<RandomAction rm (inv I e.x)(mod e.y)(sh e.z)(exc e.u)(own e.v)>
                = (inv e.x)(mod )(sh I e.z e.u)(exc )(own e.y e.v);
<RandomAction wh2 (inv e.x)(mod e.y)(sh e.z)(exc I e.u)(own e.v)>
                = (inv e.x)(mod I e.y)(sh e.z)(exc e.u)(own e.v);
<RandomAction wh3A (inv e.x)(mod e.y)(sh I e.z)(exc e.u)(own e.v)>
                = (inv e.v e.u e.z e.y e.x)(mod )(sh)(exc I)(own);
<RandomAction wh3B (inv e.x)(mod e.y)(sh e.z)(exc e.u)(own I e.v)>
                = (inv e.v e.u e.z e.y e.x)(mod )(sh)(exc I)(own);
<RandomAction wm (inv I e.x)(mod e.y)(sh e.z)(exc e.u)(own e.v)>
                = (inv e.v e.u e.z e.y e.x)(mod )(sh)(exc I)(own);
```

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

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

```
<Loop (time ) (inv e.x)(mod e.y)(sh e.z)(exc e.u)(own e.v)>
   = (inv e.x)(mod e.y)(sh e.z)(exc e.u)(own e.v);
<Loop (time s.tm e.t) (inv e.x)(mod e.y)(sh e.z)(exc e.u)(own e.v)>
   = <Loop (time e.t) <RandomAction s.tm
                           (inv e.x)(mod e.y)(sh e.z)(exc e.u)(own e.v)>>;
```

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:

$$\tau = \texttt{<Loop (time e.time) (inv I e.x)(mod)(sh)(exc)(own)>}$$

The term parameterized with two parameters `e.time` and `e.x`.

7.2 The Property of the MOESI Cache Coherence Protocol

The property of the protocol is defined with the following passive terms (see the section 3.2):

q_1 = `(inv e.x)(mod I e.y)(sh I e.z)(exc e.u)(own e.v)`,
q_2 = `(inv e.x)(mod I e.y)(sh e.z)(exc I e.u)(own e.v)`,
q_3 = `(inv e.x)(mod I e.y)(sh e.z)(exc e.u)(own I e.v)`,
q_4 = `(inv e.x)(mod e.y)(sh I e.z)(exc I e.u)(own e.v)`,
q_5 = `(inv e.x)(mod e.y)(sh e.z)(exc I e.u)(own I e.v)`,
q_6 = `(inv e.x)(mod I I e.y)(sh e.z)(exc e.u)(own e.v)`,
q_7 = `(inv e.x)(mod e.y)(sh e.z)(exc e.u)(own I 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).

7.3 The Inductive Proof

Let q be the set $\cup_i\{q_i\}$. Now we are ready to prove the safety property Q_q of the MOESI protocol with the rules defined in the section 3.2 and using the strategies described in the sections 4,5.1.

We use the same notations as in the example 1 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 $[\tau]^u$. UNFOLD rule yields $T_1 = \{\underline{[\tau]^o}, a_1^c = [\texttt{(inv I e.x)(mod)(sh)(exc)(own)}]^c,$
$a_2^u = [\texttt{<Let e.h eq <R s.m (inv I e.x)(mod)(sh)(exc)(own)> in <L (time e.t) e.h>>}]^u,$
$([\tau]^o \xrightarrow{e} a_1^c), ([\tau]^o \xrightarrow{e} a_2^u)\}$.
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 $\texttt{time} = 0$.

According the chosen strategy "call by value", UNFOLD generates (from the cases `rm, wm`) $T_2 = \{\underline{[\tau]^c}, ([\tau]^c \xrightarrow{e} a_1^c), \underline{([\tau]^c \xrightarrow{e} a_2^o)}, (a_2^o \xrightarrow{e} b_3^u), (a_2^o \xrightarrow{e} b_4^u)\}$. See the table 1 for the terms t_{b_3}, t_{b_4}.

There exist only two vertices on the path starting in the root and ending in the vertex a_2^o being considered. $\tau \not\preceq t_{a_2}$ holds. We unfold the term t_{b_3}: $T_3 =$
$\{\ldots, \underline{([\tau]^c \xrightarrow{e} a_2^c)}, \underline{(a_2^c \xrightarrow{e} b_3^o)}, (a_2^c \xrightarrow{e} b_4^u), c_5^c = [\texttt{(inv e.x)(mod)(sh I)(exc)(own)}]^c,$
$c_6^u = [\texttt{<Let e.h eq <R s.m (inv e.x)(mod)(sh I)(exc)(own)> in <L (time e.t) e.h>>}]^u,$
$(b_3^o \xrightarrow{e} c_5^c), \underline{(b_3^o \xrightarrow{e} c_6^u)}\}$.
The passive term t_{c_5} 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 $\texttt{time} = 1$. Below we omit the comments on the testing.

$\tau \not\preceq t_{b_3}$ and $t_{a_2} \not\preceq t_{b_3}$ forbid to generalize t_{b_3} and cause unfolding of t_{d_6}. We have $T_4 = \{\ldots, \underline{(a_2^c \xrightarrow{e} b_3^c)}, (a_2^c \xrightarrow{e} b_4^u), (b_3^c \xrightarrow{e} d_5^c), \underline{(b_3^c \xrightarrow{e} d_6^o)}, (c_6^o \xrightarrow{e} d_7^u), (c_6^o \xrightarrow{e} d_8^u), (c_6^o \xrightarrow{e} d_9^u)\}$.
Here the new vertices were generated from the cases `rm, wh3A, wm`. There exists the only open vertex c_6^o in T_4 and each of its ancestor $\not\preceq t_{c_6}$. That forces us to unfold t_{d_7} and the next tree is: $T_5 = \{\ldots, \underline{(b_3^c \xrightarrow{e} d_6^c)}, \underline{(d_6^c \xrightarrow{e} d_7^o)}, (d_6^c \xrightarrow{e} d_8^u),$
$(d_6^c \xrightarrow{e} d_9^u), e_{10}^c = [\texttt{(inv e.x)(mod)(sh I I)(exc)(own)}]^c,$
$e_{11}^u = [\texttt{<Let e.h eq <R s.m (inv e.x)(mod)(sh I I)(exc)(own)> in <L (time e.t) e.h>>}]^u,$
$(d_7^o \xrightarrow{e} e_{10}^c), \underline{(d_7^o \xrightarrow{e} e_{11}^u)}\}$.

It is easy to see that there exists no another possibility for the open vertex d_7^o but to take the vertex b_3^c, an ancestor of this vertex, and $t_{b_3} \preceq t_{d_7}$ holds. GENERALIZE rule constructs the term

$$g_{b_3} = \texttt{<L (time e.t)(inv e.x)(mod)(sh I e.z)(exc)(own)>}.$$

The term g_{b_3} generalizes both t_{b_3} and t_{d_7}. The next tree to be developed is:
$T_6 = \{\underline{[\tau]^c}, ([\tau]^c \xrightarrow{e} a_1^c), \underline{([\tau]^c \xrightarrow{e} a_2^c)}, \underline{(a_2^c \xrightarrow{e} b_3^u)}, (a_2^c \xrightarrow{e} b_4^u)\}$.

Note that we have replaced the term labeling the vertex b_3, but we saved the creation time of the vertex. That is a line to stress the application of GENERALIZE rule have created an new generalized induction hypothesis, i.e. a more strong hypothesis. This hypothesis together with the initial τ may be united in:

$$\texttt{<L (time e.t) (inv e.x)(mod)(sh e.z)(exc)(own)>}.$$

Hence, when we will finish the proof this more general statement (with respect to the safety of the protocol MOESI) will be proved.

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

Now we close the open vertex d_{14}^o with its ancestor b_3^c and consider its unready sibling d_{15}^u. We unfold $t_{d_{15}}$: $T_{10} = \{\ldots, (c_{13}^c \xrightarrow{e} d_{14}^c), \underline{(c_{13}^c \xrightarrow{e} d_{15}^o)}, (c_{13}^c \xrightarrow{e} d_{16}^u),$
$e_{19}^c = [\texttt{(inv e.z e.x)(mod)(sh)(exc I)(own)}]^c,$
$e_{20}^u = [\texttt{<Let e.h eq <R s.m (inv e.z e.x)(mod)(sh)(exc I)(own)> in <L (time e.t) e.h>>}]^u,$
$(d_{15}^o \xrightarrow{e} e_{19}^c), \underline{(d_{15}^o \xrightarrow{e} e_{20}^u)}\}.$

The relation $\preceq$ forbids generalization of the term $t_{d_{15}}$. We unfold $t_{e_{20}}$:
$T_{11} = \{\ldots, (d_{15}^c \xrightarrow{e} e_{19}^c), \underline{(d_{15}^c \xrightarrow{e} e_{20}^o)}, (e_{20}^o \xrightarrow{e} f_{21_1}^u), (e_{20}^o \xrightarrow{e} f_{21_2}^u), (e_{20}^o \xrightarrow{e} f_{22}^u),$
$(e_{20}^o \xrightarrow{e} f_{23_1}^u), (e_{20}^o \xrightarrow{e} f_{23_2}^u)\}$. Here the new vertices were generated from the cases `rm, wh2, wm` and we have splitted the cases `rm, wm` accordingly with SPLIT rule (the section 5.1). The term $t_{e_{20}}$ cannot be generalized. We unfold $t_{f_{21_1}}$:
$T_{12} = \{\ldots, (b_3^c \xrightarrow{e} c_{12}^c), \underline{(b_3^c \xrightarrow{e} c_{13}^c)}, (c_{13}^c \xrightarrow{e} d_{14}^c), \underline{(c_{13}^c \xrightarrow{e} d_{15}^c)}, (c_{13}^c \xrightarrow{e} d_{16}^u), (d_{15}^c \xrightarrow{e} e_{19}^c),$
$\underline{(d_{15}^c \xrightarrow{e} e_{20}^c)}, \underline{(e_{20}^c \xrightarrow{e} f_{21_1}^o)}, (e_{20}^c \xrightarrow{e} f_{21_2}^u), (e_{20}^c \xrightarrow{e} f_{22}^u), (e_{20}^c \xrightarrow{e} f_{23_1}^u), (e_{20}^c \xrightarrow{e} f_{23_2}^u),$
$h_{24}^c = [\texttt{(inv e.z e.x)(mod)(sh I I)(exc)(own)}]^c,$
$h_{25}^u = [\texttt{<Let e.h eq <R s.m (inv e.z e.x)(mod)(sh I I)(exc)(own)> in <L (time e.t) e.h>>}]^u,$
$(f_{21_1}^o \xrightarrow{e} h_{24}^c), (f_{21_1}^o \xrightarrow{e} h_{25}^u)\}.$

Now we close the open vertex $f_{21_1}^o$ with its ancestor b_3^c. The term $f_{21_2}^u$ is unfolded and closed likewise the f_{21_1}. We skip this case (T_{13}) and afterwards we have:
$T_{14} = \{\ldots, \underline{(b_3^c \xrightarrow{e} c_{13}^c)}, (c_{13}^c \xrightarrow{e} d_{14}^c), \underline{(c_{13}^c \xrightarrow{e} d_{15}^c)}, (c_{13}^c \xrightarrow{e} d_{16}^u), (d_{15}^c \xrightarrow{e} e_{19}^c), \underline{(d_{15}^c \xrightarrow{e} e_{20}^c)},$
$(e_{20}^c \xrightarrow{e} f_{21_1}^c), (e_{20}^c \xrightarrow{e} f_{21_2}^c), \underline{(e_{20}^c \xrightarrow{e} f_{22}^u)}, (e_{20}^c \xrightarrow{e} f_{23_1}^u), (e_{20}^c \xrightarrow{e} f_{23_2}^u)\}.$

UNFOLD rule applied to f_{22}^u yields:
$T_{15} = \{\ldots, (e_{20}^c \xrightarrow{e} f_{21_1}^c), (e_{20}^c \xrightarrow{e} f_{21_2}^c), \underline{(e_{20}^c \xrightarrow{e} f_{22}^o)}, (e_{20}^c \xrightarrow{e} f_{23_1}^u), (e_{20}^c \xrightarrow{e} f_{23_2}^u),$
$h_{26}^c = [\texttt{(inv e.z e.x)(mod I)(sh)(exc)(own)}]^c,$
$h_{27}^u = [\texttt{<Let e.h eq <R s.m (inv e.z e.x)(mod I)(sh)(exc)(own)> in <L (time e.t) e.h>>}]^u,$
$(f_{22}^o \xrightarrow{e} h_{26}^c), (f_{22}^o \xrightarrow{e} h_{27}^u)\}.$

The relation $\preceq$ forbids generalization of the term $t_{f_{22}}$. We unfold $t_{h_{27}}$:
$T_{16} = \{\ldots, \underline{(e_{20}^c \xrightarrow{e} f_{22}^c)}, (e_{20}^c \xrightarrow{e} f_{23_1}^u), (e_{20}^c \xrightarrow{e} f_{23_2}^u), (f_{22}^c \xrightarrow{e} h_{26}^c), \underline{(f_{22}^c \xrightarrow{e} h_{27}^o)},$

$(h^o_{27} \xrightarrow{e} i^u_{28_1}), (h^o_{27} \xrightarrow{e} i^u_{28_2}), (h^o_{27} \xrightarrow{e} i^u_{29_1}), (h^o_{27} \xrightarrow{e} i^u_{29_2})\}$. Here the new vertices were generated from the cases `rm, wm` and we have splitted these cases accordingly with SPLIT rule. The term $t_{h_{27}}$ cannot be generalized. We unfold $t_{i_{28_1}}$:
$T_{17} = \{\ldots, \underline{(f^c_{22} \xrightarrow{e} h^c_{27})}, \underline{(h^c_{27} \xrightarrow{e} i^o_{28_1})}, (h^c_{27} \xrightarrow{e} i^u_{28_2}), (h^c_{27} \xrightarrow{e} i^u_{29_1}), (h^c_{27} \xrightarrow{e} i^u_{29_2}),$
$j^c_{30} = [$`(inv e.z e.x)(mod)(sh I)(exc)(own I)`$]^c$,
$j^u_{31} = [$`<Let e.h eq <R s.m (inv e.z e.x)(mod)(sh I)(exc)(own I)> in <L (time e.t) e.h>>`$]^u$,
$(i^o_{28_1} \xrightarrow{e} j^c_{30}), \underline{(i^o_{28_1} \xrightarrow{e} j^u_{31})}\}$.

The relation $\preceq$ forbids generalization of the term $t_{i_{28_1}}$. We unfold $t_{j_{31}}$:
$T_{18} = \{\ldots, \underline{(h^c_{27} \xrightarrow{e} i^c_{28_1})}, (h^c_{27} \xrightarrow{e} i^u_{28_2}), (h^c_{27} \xrightarrow{e} i^u_{29_1}), (h^c_{27} \xrightarrow{e} i^u_{29_2}), (i^c_{28_1} \xrightarrow{e} j^c_{30}),$
$\underline{(i^c_{28_1} \xrightarrow{e} j^o_{31})}, (j^o_{31} \xrightarrow{e} k^u_{32_1}), (j^o_{31} \xrightarrow{e} k^u_{32_2}), (j^o_{31} \xrightarrow{e} k^u_{33}), (j^o_{31} \xrightarrow{e} k^u_{34}), (j^o_{31} \xrightarrow{e} k^u_{35_1}),$
$(j^o_{31} \xrightarrow{e} k^u_{35_2})\}$. Here the new vertices were generated from the cases `rm, wh3A, wh3B, wm` and we splitted the cases `rm,wm`. The term $t_{j_{31}}$ cannot be generalized. We unfold $t_{k_{32_1}}$: $T_{19} = \{\ldots, \underline{(h^c_{27} \xrightarrow{e} i^c_{28_1})}, (h^c_{27} \xrightarrow{e} i^u_{28_2}), (h^c_{27} \xrightarrow{e} i^u_{29_1}), (h^c_{27} \xrightarrow{e} i^u_{29_2}),$
$(i^c_{28_1} \xrightarrow{e} j^c_{30}), \underline{(i^c_{28_1} \xrightarrow{e} j^c_{31})}, \underline{(j^c_{31} \xrightarrow{e} k^o_{32_1})}, (j^c_{31} \xrightarrow{e} k^u_{32_2}), (j^c_{31} \xrightarrow{e} k^u_{33}), (j^c_{31} \xrightarrow{e} k^u_{34}), (j^c_{31} \xrightarrow{e} k^u_{35_1}),$
$(j^c_{31} \xrightarrow{e} k^u_{35_2}), l^c_{36} = [$`(inv e.z e.x)(mod)(sh I I)(exc)(own I)`$]^c$,
$l^u_{37} = [$`<Let e.h eq <R s.m (inv e.z e.x)(mod)(sh I I)(exc)(own I)> in <L (time e.t) e.h>>`$]^u$,
$(k^o_{32_1} \xrightarrow{e} l^c_{36}), (k^o_{32} \xrightarrow{e} l^u_{37})\}$.

Now there exists the vertex $i^c_{28_1}$, an ancestor of this vertex k^o_{32}, and $t_{i_{28_1}} \preceq t_{k_{32}}$ holds. GENERALIZE rule constructs the term

$$g_{i_{28_1}} = $`<L (time e.t)(inv e.x)(mod)(sh I e.z)(exc)(own I)>`.$$

The term $g_{i_{28_1}}$ generalizes both $t_{i_{28_1}}$ and $t_{k_{32}}$. The next tree to be developed is:
$T_{20} = \{\ldots, (f^c_{22} \xrightarrow{e} h^c_{26}), \underline{(f^c_{22} \xrightarrow{e} h^c_{27})}, \underline{(h^c_{27} \xrightarrow{e} i^u_{28_1})}, (h^c_{27} \xrightarrow{e} i^u_{28_2}), (h^c_{27} \xrightarrow{e} i^u_{29_1}),$
$(h^c_{27} \xrightarrow{e} i^u_{29_2})\}$.

Note that we have replaced the term labelling the vertex i_{28_1}. 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:
$T_{21} = \{\ldots (f^c_{22} \xrightarrow{e} h^c_{26}), \underline{(f^c_{22} \xrightarrow{e} h^c_{27})}, \underline{(h^c_{27} \xrightarrow{e} i^o_{28_1})}, (h^c_{27} \xrightarrow{e} i^u_{28_2}), (h^c_{27} \xrightarrow{e} i^u_{29_1}),$
$(h^c_{27} \xrightarrow{e} i^u_{29_2}), j^c_{38} = [$`(inv e.x1)(mod)(sh I e.z)(exc)(own I)`$]^c$,
$j^u_{39} = [$`<Let e.h eq <R s.m (inv e.x)(mod)(sh I e.z)(exc)(own I)> in <L (time e.t) e.h>>`$]^u$,
$(i^o_{28_1} \xrightarrow{e} j^c_{36}), \underline{(i^o_{28_1} \xrightarrow{e} j^u_{39})}\}$.

The relation $\preceq$ forbids generalization of the term $g_{i_{28_1}}$. We unfold $t_{j_{39}}$: $T_{22} = \{\ldots, \underline{(h^c_{27} \xrightarrow{e} i^c_{28_1})}, (h^c_{27} \xrightarrow{e} i^u_{28_2}), (h^c_{27} \xrightarrow{e} i^u_{29_1}), (h^c_{27} \xrightarrow{e} i^u_{29_2}), (i^c_{28_1} \xrightarrow{e} j^c_{36}), \underline{(i^c_{28_1} \xrightarrow{e} j^o_{39})},$
$(j^o_{39} \xrightarrow{e} k^u_{40}), (j^o_{39} \xrightarrow{e} k^u_{41}), (j^o_{39} \xrightarrow{e} k^u_{42}), (j^o_{39} \xrightarrow{e} k^u_{43})\}$. Here the new vertices were generated from the cases `rm,wh3A,wh3B,wm`. The term $t_{j_{39}}$ cannot be generalized. We unfold $t_{k_{40}}$: $T_{23} = \{\ldots, \underline{(h^c_{27} \xrightarrow{e} i^c_{28_1})}, (h^c_{27} \xrightarrow{e} i^u_{28_2}), (h^c_{27} \xrightarrow{e} i^u_{29_1}), (h^c_{27} \xrightarrow{e} i^u_{29_2}),$
$(i^c_{28_1} \xrightarrow{e} j^c_{36}), \underline{(i^c_{28_1} \xrightarrow{e} j^c_{39})}, \underline{(j^c_{39} \xrightarrow{e} k^o_{40})}, (j^c_{39} \xrightarrow{e} k^u_{41}), (j^c_{39} \xrightarrow{e} k^u_{42}), (j^c_{39} \xrightarrow{e} k^u_{43}),$

$l^c_{44} = [$`(inv e.x)(mod)(sh I I e.z)(exc)(own I)`$]^c$,
$l^u_{45} = [$`<Let e.h eq <R s.m (inv e.x)(mod)(sh I I e.z)(exc)(own I)>`
`in <L (time e.t) e.h>>`$]^u$,
$(k^o_{40} \xrightarrow{e} l^c_{44}), (k^o_{40} \xrightarrow{e} l^u_{45})\}$.

Here we close the open vertex k^o_{40} with $i^c_{28_1}$ and unfold its sibling $t_{k_{41}}$:
$T_{24} = \{\ldots, \underline{(i^c_{28_1} \xrightarrow{e} j^c_{39})}, (j^c_{39} \xrightarrow{e} k^c_{40}), \underline{(j^c_{39} \xrightarrow{e} k^o_{41})}, (j^c_{39} \xrightarrow{e} k^u_{42}), (j^c_{39} \xrightarrow{e} k^u_{43}),$
$l^c_{46} = [$`(inv I e.z e.x)(mod)(sh)(exc I)(own)`$]^c$,
$l^u_{47} = [$`<Let e.h eq <R s.m (inv I e.z e.x)(mod)(sh)(exc I)(own)>`
`in <L (time e.t) e.h>>`$]^u$,
$(k^o_{41} \xrightarrow{e} l^c_{46}), (k^o_{41} \xrightarrow{e} l^u_{47})\}$.

Here we close the vertex k^o_{41} with d^c_{15} and consider its sibling k^u_{42}. $t_{k_{41}} = t_{k_{42}}$ implies the vertex k^u_{42} can be unfolded and closed likewise k^u_{41}. We omit the development of k^u_{42} (T_{25}) and consider its sibling k^u_{43}. $t_{k_{43}} \ll t_{k_{41}}$ implies the vertex k^u_{43} can be unfolded and closed likewise k^u_{41}. We omit its development (T_{26}). The vertex k^u_{43} is the last from its siblings and we have reached a bottom of the tree of all possible cases.

Analysis of the remaining variants Accordingly with our depth first strategy (the section 4) we have to consider the remaining variants in the order of decreasing of their creation times. The current tree looks as follows:
$T_{27} = \{\ldots, \underline{(f^c_{22} \xrightarrow{e} h^c_{27})}, \underline{(h^c_{27} \xrightarrow{e} i^c_{28_1})}, (h^c_{27} \xrightarrow{e} i^u_{28_2}), (h^c_{27} \xrightarrow{e} i^u_{29_1}), (h^c_{27} \xrightarrow{e} i^u_{29_2}),$
$(i^c_{28_1} \xrightarrow{e} j^c_{36}), \underline{(i^c_{28_1} \xrightarrow{e} j^c_{39})}, (j^c_{39} \xrightarrow{e} k^c_{40}), (j^c_{39} \xrightarrow{e} k^c_{41}), (j^c_{39} \xrightarrow{e} k^c_{42}), \underline{(j^c_{39} \xrightarrow{e} k^c_{43})}\}$.

We see the next vertex to be unfolded is the second child of h^c_{27}. We denote the completely closed part of the tree as T_c and unfold the term $t_{i_{28_2}}$:
$T_{28} = \{\ldots, \underline{(f^c_{22} \xrightarrow{e} h^c_{27})}, (h^c_{27} \xrightarrow{e} i^c_{28_1}), \underline{(h^c_{27} \xrightarrow{e} i^o_{28_2})}, (h^c_{27} \xrightarrow{e} i^u_{29_1}), (h^c_{27} \xrightarrow{e} i^u_{29_2}), T_c,$
$j^c_{48} = [$`(inv e.x)(mod)(sh I)(exc)(own I)`$]^c$,
$j^u_{49} = [$`<Let e.h eq <R s.m (inv e.x)(mod)(sh I)(exc)(own I)>`
`in <L (time e.t) e.h>>`$]^u$,
$(i^o_{28_2} \xrightarrow{e} j^c_{48}), (i^o_{28_2} \xrightarrow{e} j^u_{49})\}$.

We close the open vertex $i^o_{28_2}$ with $i^c_{28_1}$ [6] and unfold its sibling $t_{i_{29_1}}$:
$T_{29} = \{\ldots, \underline{(c^c_{13} \xrightarrow{e} d^c_{15})}, (c^c_{13} \xrightarrow{e} d^u_{16}), (d^c_{15} \xrightarrow{e} e^c_{19}), \underline{(d^c_{15} \xrightarrow{e} e^c_{20})}, (e^c_{20} \xrightarrow{e} f^c_{21_1}),$
$(e^c_{20} \xrightarrow{e} f^c_{21_2}), \underline{(e^c_{20} \xrightarrow{e} f^c_{22})}, (e^c_{20} \xrightarrow{e} f^u_{23_1}), (e^c_{20} \xrightarrow{e} f^u_{23_2}), (f^c_{22} \xrightarrow{e} h^c_{26}), \underline{(f^c_{22} \xrightarrow{e} h^c_{27})},$
$(h^c_{27} \xrightarrow{e} i^c_{28_1}), (h^c_{27} \xrightarrow{e} i^c_{28_2}), \underline{(h^c_{27} \xrightarrow{e} i^o_{29_1})}, (h^c_{27} \xrightarrow{e} i^u_{29_2}), T_c,$
$j^c_{50} = [$`(inv I e.z e.x)(mod)(sh)(exc I)(own)`$]^c$,
$j^u_{51} = [$`<Let e.h eq <R s.m (inv I e.z e.x)(mod)(sh)(exc I)(own)>`
`in <L (time e.t) e.h>>`$]^u$,
$(i^o_{29_1} \xrightarrow{e} j^c_{50}), (i^o_{29_1} \xrightarrow{e} j^u_{51})\}$.

We close the open vertex $i^o_{29_1}$ with d^c_{15} and consider its sibling $i^u_{29_2}$. $t_{i_{29_2}} \ll t_{i_{29_1}}$ implies the vertex $i^u_{29_2}$ can be unfolded and closed likewise i_{29_1}. We omit its development (T_{30}). The vertex $i^u_{29_2}$ is the last from its siblings and we have reached a next bottom of the tree of all possible cases. Now the next vertices to be developed are the siblings $f^u_{23_1}$ and $f^u_{23_2}$. They similar to i_{29_1}, i_{29_2} considered

[6] Recall the vertex $i^c_{28_1}$ was generalized.

above and we omit closing the siblings (T_{31}). Denote the closed part of the tree as T_{c_1}. We have: $T_{32} = \{\dots, \underline{(b_3^c \xrightarrow{e} c_{13}^c)}, (c_{13}^c \xrightarrow{e} d_{14}^c), (c_{13}^c \xrightarrow{e} d_{15}^c), \underline{(c_{13}^c \xrightarrow{e} d_{16}^u)}, T_{c_1}\}$.

The next term to be unfolded is $t_{d_{16}}$: $T_{33} = \{\dots, \underline{(b_3^c \xrightarrow{e} c_{13}^c)}, (c_{13}^c \xrightarrow{e} d_{14}^c),$
$(c_{13}^c \xrightarrow{e} d_{15}^c), \underline{(c_{13}^c \xrightarrow{e} d_{16}^o)}, T_{c_1}, e_{52}^c = [$`(inv I e.z e.x)(mod)(sh)(exc I)(own)`$]^c,$
$e_{53}^u = [$`<Let e.h eq <R s.m (inv I e.z e.x)(mod)(sh)(exc I)(own)>`
`in <L (time e.t) e.h>>`$]^u,$
$(d_{16}^o \xrightarrow{e} e_{52}^c), (d_{16}^o \xrightarrow{e} e_{53}^u)\}$.

We close the open vertex d_{16}^o with d_{15}^c. The next vertex to be unfolded is b_4^u:
$T_{34} = \{\dots, \underline{(a_2^c \xrightarrow{e} b_4^o)}, (b_3^c \xrightarrow{e} c_{12}^c), (b_3^c \xrightarrow{e} c_{13}^c), (c_{13}^c \xrightarrow{e} d_{14}^c), (c_{13}^c \xrightarrow{e} d_{15}^c), (c_{13}^c \xrightarrow{e} d_{16}^c),$
$T_{c_1}, c_{54}^c = [$`(inv e.x)(mod)(sh)(exc I)(own)`$]^c,$
$c_{55}^u = [$`<Let e.h eq <R s.m (inv e.x)(mod)(sh)(exc I)(own)>`
`in <L (time e.t) e.h>>`$]^u,$
$(b_4^o \xrightarrow{e} c_{54}^c), (b_4^o \xrightarrow{e} c_{55}^u)\}$.

We close the open vertex b_4^o with d_{15}^c:
$T_{35} = \{[\tau]^c, ([\tau]^c \xrightarrow{e} a_1^c), ([\tau]^c \xrightarrow{e} a_2^c), (a_2^c \xrightarrow{e} b_3^c), (a_2^c \xrightarrow{e} b_4^c), (b_3^c \xrightarrow{e} c_{12}^c), (b_3^c \xrightarrow{e} c_{13}^c),$
$(c_{13}^c \xrightarrow{e} d_{14}^c), (c_{13}^c \xrightarrow{e} d_{15}^c), (c_{13}^c \xrightarrow{e} d_{16}^c), T_{c_1}\}$.

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

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

τ = <L (time e.time)(inv I e.x)(mod)(sh)(exc)(own)>
t_{b_3} = <L (time e.t)(inv e.x)(mod)(sh I)(exc)(own)> g_{b_3} = *<L (time e.t)(inv e.x)(mod)(sh I e.z)(exc)(own)>* t_{b_4} = <L (time e.t)(inv e.x)(mod)(sh)(exc I)(own)>
t_{d_7} = <L (time e.t)(inv e.x)(mod)(sh I I)(exc)(own)> t_{d_8} = <L (time e.t)(inv e.x)(mod)(sh)(exc I)(own)> t_{d_9} = <L (time e.t)(inv I e.x)(mod)(sh)(exc I)(own)> $t_{d_{14}}$ = <L (time e.t)(inv e.x)(mod)(sh I I e.z)(exc)(own)> $t_{d_{15}}$ = <L (time e.t)(inv e.z e.x)(mod)(sh)(exc I)(own)> $t_{d_{16}}$ = <L (time e.t)(inv I e.z e.x)(mod)(sh)(exc I)(own)>
$t_{f_{21_1}}$ = <L (time e.t)(inv e.z e.x)(mod)(sh I I)(exc)(own)> $t_{f_{21_2}}$ = <L (time e.t)(inv e.x)(mod)(sh I I)(exc)(own)> $t_{f_{22}}$ = <L (time e.t)(inv e.z e.x)(mod I)(sh)(exc)(own)> $t_{f_{23_1}}$ = <L (time e.t)(inv I e.z e.x)(mod)(sh)(exc I)(own)> $t_{f_{23_2}}$ = <L (time e.t)(inv I e.x)(mod)(sh)(exc I)(own)>
$t_{i_{28_1}}$ = <L (time e.t)(inv e.z e.x)(mod)(sh I)(exc)(own I)> $g_{i_{28_1}}$ = *<L (time e.t)(inv e.x)(mod)(sh I e.z)(exc)(own I)>* $t_{i_{28_2}}$ = <L (time e.t)(inv e.x)(mod)(sh I)(exc)(own I)> $t_{i_{29_1}}$ = <L (time e.t)(inv I e.z e.x)(mod)(sh)(exc I)(own)> $t_{i_{29_2}}$ = <L (time e.t)(inv I e.x)(mod)(sh)(exc I)(own)>
$t_{k_{32_1}}$ = <L (time e.t)(inv e.z e.x)(mod)(sh I I)(exc)(own I)> $t_{k_{32_2}}$ = <L (time e.t)(inv e.x)(mod)(sh I I)(exc)(own I)> $t_{k_{33}}$ = <L (time e.t)(inv I e.z e.x)(mod)(sh)(exc I)(own)> $t_{k_{34}}$ = <L (time e.t)(inv I e.z e.x)(mod)(sh)(exc I)(own)> $t_{k_{35_1}}$ = <L (time e.t)(inv I I e.z e.x)(mod)(sh)(exc I)(own)> $t_{k_{35_2}}$ = <L (time e.t)(inv I I e.x)(mod)(sh)(exc I)(own)> $t_{k_{40}}$ = <L (time e.t)(inv e.x)(mod)(sh I I e.z)(exc)(own I)> $t_{k_{41}}$ = <L (time e.t)(inv I e.z e.x)(mod)(sh)(exc I)(own)> $t_{k_{42}}$ = <L (time e.t)(inv I e.z e.x)(mod)(sh)(exc I)(own)> $t_{k_{43}}$ = <L (time e.t)(inv I I e.z e.x)(mod)(sh)(exc I)(own)>

Table 1. MOESI configurations.

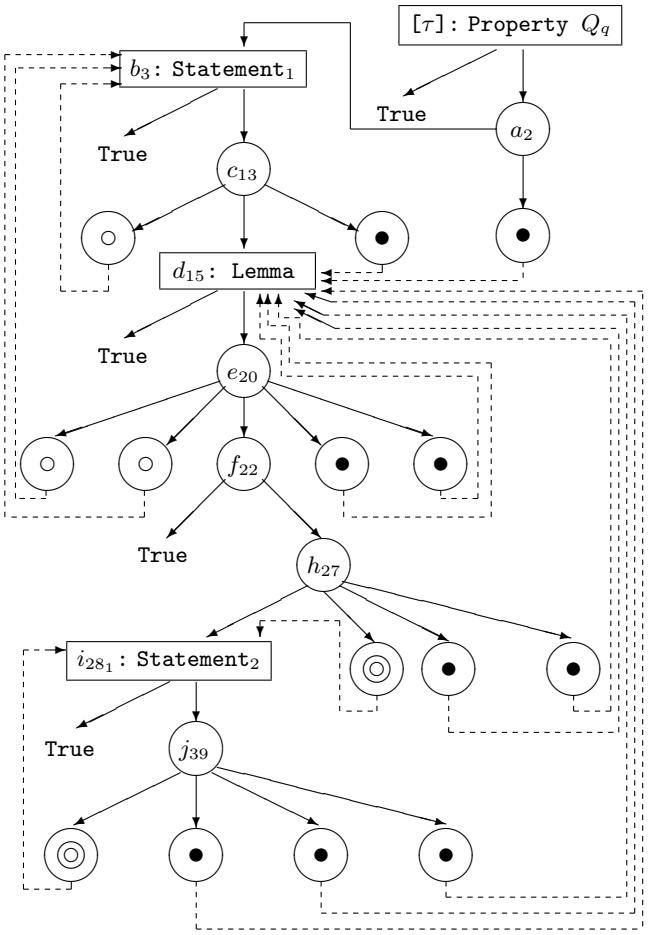

Fig. 1. Graph of the automatic proof.